# Exhibit 1: Version 2.4

**Texas Department of Information Resources**

## Data Center Services Program

## Security Operations Services

## Statement of Work

## Table of Contents

## TABLE OF DOCUMENTS

**RFO**

Attachment 1: Respondent Information Form

Attachment 2: HUB Subcontracting Plan

Attachment 6: Respondent Release of Liability

**Master Services Agreement (MSA)**

Attachment 1: Form of Nondisclosure

Attachment 2: Insurance and Risk of Loss

Attachment 3: Form of Source Code Escrow (if applicable)

**Exhibit 1 Security Operations Services Statement of Work (Exhibit 1 SOW)** (this document)

**Attachments**

Attachment 1.1: Deliverables
Attachment 1.2: Service Level Matrix
Attachment 1.3: Service Level Definitions and Performance Analytics
Attachment 1.4: SMM Content and Organization
Attachment 1.5: Key Personnel

**Appendices**

Appendix A – Reports

**Exhibit 2 Security Operations Services Financial Provisions and Pricing (Exhibit 2 Pricing)**

Attachment 2.1: Pricing and Volumes
Attachment 2.2: Financial Responsibility Matrix

**Table 1: Terms and Definitions**

| Term | Definition |
|---|---|
| Acceptance or Accepted | The determination, in the Department of Information Resources (DIR) or, if applicable, DCS Customers' reasonable discretion and in accordance with the relevant provisions of Article 10 Contract Management, confirmed in writing by DIR or the applicable DCS Customer, that Software, Equipment, Systems, and/or other Deliverables are in Compliance, in accordance with **Master Services Agreement (MSA), Section 8.4.3 Developed Materials Compliance** and the **Services Management Manual (SMM)** or other criteria agreed to in writing by the Parties. |
| Acceptance Criteria | The criteria that Successful Respondent must confirm have been met prior to submitting a Deliverable or Milestone for Acceptance by DIR or a DCS Customer. Acceptance Criteria include: (i) any mutually agreed written criteria identified as Acceptance Criteria, (ii) Compliance, (iii) for all Software and System deliverables that process data, such item successfully integrates with all other Services, Software, Equipment, Systems, and other resources and is fully documented such that the anticipated end user can utilize the functionality of such Deliverable in the manner and for the purpose intended and that reasonable knowledgeable professionals can understand, maintain, support, and modify such Deliverable in accordance with its intended use. |
| Acceptance Review Period | Has the meaning given in Section 10.6 Acceptance Review Period, provided that any provisions of written notice alerting DIR that a Milestone or Deliverable is complete and ready for review that is submitted outside a Business Day shall be considered to be submitted, for the purposes of DIR internal review, on the next Business Day immediately following the day on which such notice was submitted. |
| ADC | Austin Data Center. |
| ADDF | Application Development Decision Framework – High level information about the ADDF is available at this link: https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Texas%20ADDF%20Pamphlet.pdf |
| Administration Services | The act of managing planning, directing, and coordinating supportive services for an activity and/or organization. |
| Affiliate | With respect to an Entity, any other Entity that directly or indirectly Controls, is Controlled by, or is under common Control with that Entity at the time in question. |
| Agreement (also Master Services Agreement and MSA and Contract) | The final version of any contractually binding agreement between DIR and the Successful Respondent relating to the subject matter of the RFO; references to the Agreement include all Exhibits, Attachments and other documents attached thereto or incorporated therein by reference.<br>Notwithstanding the foregoing, unless expressly provided or the context otherwise requires, references to the Agreement in conjunction with Section or Article references shall be deemed references to the body of the Agreement. |
| AIMS | Asset Inventory and Management System. |
| Allocation of Pool Percentage | The portion of the respective Pool Percentage Available for Allocation that is specified for a Performance Category. The total of all Allocation of Pool Percentages shall not exceed the Pool Percentage Available for Allocation. |
| API | Application Programming Interface. |

| Term | Definition |
|---|---|
| Appliances | A specialized computing device with pre-integrated and pre-configured hardware and/or software packaged to provide a "turn-key" solution. The computing function in an Appliance, though configurable, is designed by the manufacturer to provide a specific function with little or no support. Computer appliances differ from general purpose computers such as an Application or Infrastructure Server in that they are not designed to be modified. Appliances may be physical or virtual and support a variety of functions. |
| Applications | All software programs and programming (and all modifications, replacements, Upgrades, enhancements, documentation, materials, media, on-line help documentation and tools related thereto) that perform user or DCS Customer-related information processing functions or support day- to-day operations (including the supporting documentation, media, on- line help facilities, and tutorials), or otherwise used in the provision of Services by Successful Respondent. Applications include all such programs and programming in use or required to be used as of the Commencement Date. Applications also include all such programs and programming developed and/or introduced by or for DIR, any DCS Customer, or Successful Respondent during the Term. Applications do not include the tools, utilities, or Operating Software or Systems Software used to deliver Applications. |
| Architecture | The design, process, strategies, and specification of the overall structure, logical components, and the logical interrelationships of Equipment and Software, including System Software, a Network, or other reasonably related conception. |
| Assessment(s) or Assessed | Has the meaning given in Section 9.8.11.8 Security Assessments. |
| Assessment Notice Date | The date that DIR or the Security Assessment Company, as applicable, provides an Assessment report to Successful Respondent. |
| Asset Inventory and Management System (AIMS) | An automated, database-driven application used to store, query, and maintain asset inventory information for all assets used in association with the Services, whether the assets are located at DIR Facilities or Successful Respondent Facilities. The AIMS provides an inventory of the IT infrastructure managed by the Successful Respondent. |
| Assistance Event | (i) Any termination (in whole or in part) under, or the expiration of, the Agreement, or (ii) The discontinuance of the provision of the Services (in whole or in part) in respect of any DCS Customer. |
| At-Risk Amount | For any month during the Term, the percent (%) of the Service Level Invoice Amount, which is the maximum amount that the Successful Respondent will have at risk for Service Level Credits as set forth in **Attachment 1.1 Deliverables.** Each Service Component will have its own At-Risk Amount tied to the corresponding portion of the Service Level Invoice Amount. See the formula in **Attachment 1.1 Deliverables, Section 6.5**. |
| Audit Period | Has the meaning given in **MSA, Section 4.11.1 Contract Records**. |
| Authorized Users | Unless otherwise indicated, officers, directors, employees, contractors, agents, customers, and vendors of DIR or any DCS Customer and any other person(s) designated by DIR or any DCS Customer to receive or use the Systems or Services provided by Successful Respondent. |
| Availability or Available | The full functionality of a Service Component is ready and accessible for use by the Authorized Users and is not degraded in any material respect. |
| Bankruptcy Code | Has the meaning given in **MSA, Section 13.5.2 DIR Rights in Event of Bankruptcy Rejection**. |
| Bankruptcy Rejection | Has the meaning given in **MSA, Section 13.5.2 DIR Rights in Event of Bankruptcy Rejection**. |
| BC | Business Continuity. |

| Term | Definition |
|---|---|
| Business Continuity | The overall enterprise plans and specific activities of each DCS Customer and/or Service Component Provider (SCP) that are intended to enable continued business operations in the event of any unforeseen interruption (e.g., plans and activities to move a department to a new location in the event of a disruption). |
| Business Day | Each day from Monday through Friday, excluding State holidays, 7:00 a.m. to 5:00 p.m., Local Time. State holidays will include all holidays with the status "All agencies closed." State holidays will not include State optional holidays or holidays that require skeleton crews.<br><br>For SLAs related to outbound mail Services, Business Day means each day from Monday through Friday, excluding US postal holidays, 7:00 a.m. to 5:00 p.m., Local Time. For SLA reporting purposes, the hours listed **in Attachment 1.3 Service Level Definitions and Performance Analytics** would override the 7:00 a.m. to 5:00 p.m. |
| Cabling | The physical connection between pieces of equipment that are generally loose, not necessarily permanent and attached to infrastructure (e.g. within racks and cabinets). |
| Call | A contact (including by telephone, voicemail, electronic mail, fax, automated tool or web request) to Successful Respondent reporting a problem, requesting assistance or Services, or asking a question pertaining to the Services, as well as automated alerts and other problem and Service notifications communicated to Successful Respondent. |
| CAP Failure Credit | Has the meaning given in Section 6.8 Service Delivery Failure: Corrective Action Plan. |
| CDC | Consolidated Data Center (inclusive of both ADC and SDC). |
| Change Control Procedures | Has the meaning given in **MSA, Section 4.9 Change Control**. |
| Change Management or Change Management Process | The processes relating to planning and performing all changes in DCS Customer's IT environment pertaining to the Services, including changes to individual components and coordination of changes across all components. The Change Management processes will support and include checkpoints to determine any potential or required Change Control Procedures. |
| Chargeback | Has the meaning given in **Exhibit 2 Pricing**. |
| Chargeback System | The system for Chargeback as described in **Exhibit 2 Financial Provisions and Pricing, Section 2.3**. |
| Charges | The Monthly Base Charge, Additional Resource Charges and any other amounts payable by DIR to Successful Respondent pursuant to the express terms of the Agreement. |
| CI | Configuration Items; any component part of Services that is (or is to be) under the control of Configuration Management and therefore subject to formal Change Control. |
| CJIS | Criminal Justice Information Services. |
| Cloud | Shared pools of configurable computer system resources and higher-level services that can be rapidly provisioned with minimal management effort, often over the Internet. Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a public utility. |
| CMDB | Configuration Management Database is a database used by an organization to store information about hardware and software assets. This database acts as a data warehouse for the organization and also stores information regarding the relationship between its assets. |

| Term | Definition |
|---|---|
| CMS | Configuration Management System. A system engineering process for establishing and maintaining consistency of a product's performance, functional, and physical attributes with its requirements, design, and operational information throughout its life. |
| Commencement Date | September 1, 2020, or the date the Parties agree upon, in writing, as the date on which Successful Respondent begins providing the Services to the first DCS Customer. |
| Compliance and Comply | With respect to Deliverables, fulfilling the requirements of the specifications, the Acceptance Criteria, the Agreement, and all other applicable operational and/or functional requirements. |
| Component | A grouping of software functionally or a separate software object in the solution that has the ability to "stand alone" or "integrate with other components" as required. |
| Confidential Information | Has the meaning given in **MSA, Section 6.1.1 Confidential Information.** |
| Configuration Item (CI) | Any component part of Services that is (or is to be) under the control of Configuration Management and therefore subject to formal Change Control. |
| Configuration Management Database (CMDB) | A System that contains details regarding the Software, Equipment and Systems that are used in the provision and management of the Services, including information that relates to the maintenance, movement and problems experienced with such Software, Equipment and Systems. |
| Connectivity | The ability to access and exchange data, voice, and/or video electronic impulses between various Infrastructure components and with external sources as approved by DIR and provided to Authorized Users. |
| Consolidated Data Center(s) | Means the centralized Data Center(s) used by Successful Respondent to provide Services (including the ADC and SDC). |
| Contract Changes | Has the meaning given in Section 10.1 Contract Changes. |
| Contract Records | Has the meaning given in **MSA, Section 4.11.1 Contract Records.** |
| Contract Year | Each twelve (12) month period commencing each September and ending each August during the Term. If any Contract Year is less than twelve (12) months ("Stub Period"), the rights and obligations under this Agreement that are calculated on a Contract Year basis will be proportionately adjusted for such shorter period. |
| Contract | See "Agreement". |
| Control, Controlled and Controlling | Means (a) the legal, beneficial, or equitable ownership, directly or indirectly, of (i) at least fifty percent (50%) of the aggregate of all voting equity interests in an Entity, or (ii) equity interests having the right to at least fifty percent (50%) of the profits of an Entity or, in the event of dissolution, to at least fifty percent (50%) of the assets of an Entity; (b) the right to appoint, directly or indirectly, a majority of the board of directors; (c) the right to control, directly or indirectly, the management or direction of the Entity by contract or corporate governance document; or (d) in the case of a partnership, the holding by an Entity (or one of its Affiliates) of the position of sole general partner. For purposes of this Agreement, a Change in Control under **MSA, Section 13.3** occurs if the ultimate parent entity no longer Controls (as described above) Successful Respondent. |
| Corrective Action Plan or CAP | Has the meaning given in Section 6.7.1 Additions. |
| CPU | Central Processing Unit. |

| Term | Definition |
|---|---|
| Critical Deliverable | Deliverables that have associated Deliverable Credits payable to DIR in the event Successful Respondent fails to successfully and timely complete such Deliverables as identified in the Agreement. For further clarity, successfulness is measured by whether the Deliverables meet the associated Acceptance Criteria. |
| Critical Milestone(s) | The event(s) that evidence that progress has been made and that specific action(s) has taken place in the advancement of work. Usually viewed as a significant achievement or attainment of a specific goal or sub-goal. |
| Critical Service Level | Any Service Level designated as "critical" by DIR, and with respect to which DIR may become entitled to receive Service Level Credits as a result of Successful Respondent's failure to satisfy the associated Service Level standards. |
| Cross-Functional Services | Those Services performed in connection with performing, and in support of, each of the Services, including those Services described in Article 9 Cross-Functional Services. |
| CSP | Cloud Service Provider. |
| Data Quality Management (DQM) | The business processes that ensure the integrity of an organization's data during collection, application (including aggregation), warehousing, and analysis. |
| DCS | Data Center Services. |
| DCS Customer or DCS Customer | Collectively, any of the following Entities that are designated by DIR to receive Services under the Agreement, whether directly from any DCS Service Component Provider or from DIR through an Interagency, Interlocal, or other agreement: (a) DIR in its capacity as a recipient of Services; (b) any State agency, unit of local government or institution of higher education as defined in Section 2054.003, Texas Government Code, and those State agencies that execute Interagency Agreements with DIR, as authorized by Chapter 771, Texas Government Code; (c) any Texas local government as authorized through the Interlocal Cooperation Act, Chapter 791, Texas Government Code; (d) any other state or governmental Entity of another state, as authorized by Section 2054.0565, Texas Government Code; (e) any other Entity permitted under Law to purchase Services from or through DIR; and (f) other Entities to which the Parties agree. The Parties acknowledge and agree that the definition of eligible DCS Customers is subject to modification by the State Legislature, and that the then-current definition of DCS Customers shall control for all purposes. |
| DCS Governance Model | Has the meaning given in Article 8 DCS Governance Model. |
| DCS Network or Managed DCS Network Services | The DCS Service Component providing Network support and services. It is a DCS Shared Technology Service (STS) that will be provided by an SCP. One (1) of several Service Components comprising the DCS Program. |
| DCS Prospects | Potential Data Center Services clients. |
| DCS Security Operations Services (SOS) | The DCS Service Component for Security. It is a DCS STS that will be provided by an SCP. One (1) of several Service Components comprising the DCS Program. |
| DCS Service Component Provider(s) | Collectively, all Service Component Providers and the MSI. |

| Term | Definition |
|---|---|
| Deliverable | In accordance with Section 10.2 Deliverables, a vendor-provided tangible item or outcome that DIR reviews and approves at a specified date/frequency during the term of the contract, excluding reports that are managed/monitored through other defined processes. Deliverables may have certain attributes that impact the review and acceptance. The term includes Recurring and One-Time Deliverables. |
| Deliverable Credits | Has the meaning given in Section 10.10 Deliverables Credits. |
| Derivative Work | A work based on one or more preexisting works, including a condensation, transformation, translation, modification, expansion, or adaptation, that, if prepared without authorization of the owner of the copyright of such preexisting work, would constitute a copyright infringement under applicable Laws, but excluding the preexisting work. |
| Designated DIR Representative | Has the meaning given in **MSA, Section 5.1.1 Designated DIR Representative**. |
| Developed Material(s) | Any Materials or any modifications, enhancements, improvements, Upgrades or Derivative Works of such Materials that are developed pursuant to the Agreement and paid for by DIR or any DCS Customer under the Agreement. Developed Materials does not include any underlying Successful Respondent or Third Party Owned Materials. |
| Development or Development Environment | The Systems environment in which Software and databases are initially designed and created. DCS Customers may have more than one Development Environment. |
| DevOps | A set of software development practices that combine software development (Dev) and information technology operations (Ops) to shorten the systems development life cycle while delivering features, fixes, and updates frequently in close alignment with business objectives. |
| DIR | Department of Information Resources. |
| DIR Auditors | Has the meaning given in **MSA, Section 4.11.2 Operational Audits**. |
| DIR Business Days | Means weekdays (Monday through Friday) excluding State of Texas and Federal holidays. The term does not include weekends. |
| DIR Contractor(s) | Has the meaning as the term is used in **MSA, Article 4 Services**. |

| Term | Definition |
|---|---|
| DIR Data | Any data or information of or regarding DIR or any DCS Customer that is provided to or obtained by Successful Respondent in connection with the negotiation and execution of the Agreement or the performance of Successful Respondent's obligations under the Agreement, including data and information with respect to the constituency, customer, operations, facilities, products, rates, regulatory compliance, competitors, assets, expenditures, mergers, acquisitions, divestitures, billings, collections, revenues and finances of DIR or any DCS Customer. DIR Data also means any data or information:<br><br>1. created, generated, collected or processed by Successful Respondent in the performance of its obligations under the Agreement, including data processing input and output, service level measurements, asset information, Reports, third party service and product agreements, contract charges, and retained expense and Pass-Through Expenses;<br>2. that resides in or is accessed through Software, Equipment or Systems provided, operated, supported, or used by Successful Respondent in connection with the Services, as well as information derived from this data and information, but excluding the following information to the extent not required to be provided or otherwise made available to DIR under this Agreement, including with in connection with DIR's rights related to Benchmarking, Subcontractors, auditing, Reports, or Termination Assistance Services: financial/accounting information (including costs, expenditures, billings collections, revenues and finances) of Successful Respondent, its Affiliates or Subcontractors;<br>3. information created by Successful Respondent to measure the productivity and efficiency of the Services and/or to improve the processes and procedures used by in the performance of the Services;<br>4. human resources and personnel information of Successful Respondent, its Affiliates or Subcontractors; and<br>5. information with respect to Third Party Contracts or licenses of Successful Respondent, its Affiliates or Subcontractors and used in the performance of the Services.<br><br>Data or information constituting DIR Data shall not constitute Successful Respondent Confidential Information. |
| DIR Facilities or DIR Facility | The facilities that are provided by DIR or a DCS Customer for use by Successful Respondent to the extent necessary to provide the Services as well as those DIR, DCS Customer and DIR Contractor locations at or to which Successful Respondent is to provide the Services. DIR Facilities include the Non-Consolidated Service Locations and the Consolidated Data Centers. |
| DIR Laws | Has the meaning given in **MSA, Section 8.11.4 Notice of Laws**. |
| DIR Owned Materials | Has the meaning given in **MSA, Section 7.1 DIR Owned and Licensed Materials**. |
| DIR Personal Data | That portion of DIR Data that is subject to any Privacy Laws and includes, but is not limited to, information which any DCS Customer discloses that consists of personal Confidential Information or identifies any consumer served by the Texas Health and Human Services Commission or constituent agencies, in accordance with applicable federal and state laws and other applicable rules, including but not limited to the Texas Health and Safety Code and 25 Texas Administrative Code, Chapter 414. |

| Term | Definition |
|---|---|
| DIR Project Manager | The person or the person's designee identified by DIR as the responsible individual from DIR to manage the project. |
| DIR Rules | Has the meaning given in **MSA, Section 4.3 DIR Rules/Employee Safety**. |
| DIR Standards or Standards | Has the meaning given in **MSA, Section 4.9 Change Control**. |
| DIR-Initiated Financial Dispute | Has the meaning given in **Exhibit 2 Financial Provisions and Pricing**, **Section 2.2.4.3.** |
| Disaster | (1) A sudden, unplanned calamitous event causing great damage or loss; (2) any event that creates an inability on an organizations part to provide critical business functions for some predetermined period of time; (3) in the business environment, any event that creates an inability on an organization's part to provide the critical business functions for some predetermined period of time; (4) the period when company management decides to divert from normal production responses (in total or in part) and exercises its disaster recovery plan; and (5) typically signifies the beginning of a move from a primary to an alternate location. |
| Disaster Recovery (DR) Services | The process of following specific advance arrangements and procedures in response to a disaster, resumption of the critical business functions within a predetermined period of time, minimizing the amount of loss, and repairing or replacing the damaged facilities as soon as possible. The Disaster Recovery Services include support and coordination with the Business Continuity Services. |
| Disaster Recovery Plan (DRP) | The plan to execute Disaster Recovery Services. |
| Downtime | The time that a particular System, Application, Software, Equipment, Network or any other part of the Services is not Available during the Measurement Window. |
| DR | Disaster Recovery. |
| DRP | Disaster Recovery Plan. |
| Earnback | The methodology used to determine the potential return of a Service Level Credit as described in Section 6.6 Earnback. |
| Effective Date | Has the meaning given in the "Authority to Execute" Section of the Agreement, which is understood to be the day the final party signs the Agreement. |
| Electronic PHI or ePHI | Has the meaning given in **MSA, Section 6.3 DIR Personal Data**. |
| Eligible Customer(s) | See DCS Customers. |
| Entity or Entities | A governmental body, agency, unit or division (including those categories described in the definition of DCS Customer), corporation, partnership, joint venture, trust, limited liability company, limited liability partnership, association, or other organization or entity. |

| Term | Definition |
|---|---|
| Equipment | The computer, telecommunications, and facility-related hardware, equipment, and peripherals (and all modifications, replacements, Upgrades, enhancements, documentation, materials, and media related thereto) that are used in connection with the Services provided by Successful Respondent. Equipment includes all such computer, telecommunications, and facility-related hardware, equipment, and peripherals in use or required to be used as of the Commencement Date, including those set forth in the Agreement; those as to which the lease, maintenance, or support costs are included in the Financial Base Case; and those as to which Successful Respondent received reasonable notice and/or access prior to the Commencement Date. Equipment also includes all such computer, telecommunications, and facility-related hardware, equipment, and peripherals purchased or leased by or for DIR, any DCS Customer, or Successful Respondent during the Term. |
| Equipment Lease | All leasing arrangements whereby DIR, DCS Customers, or any DIR Contractor leases Equipment as of the Commencement Date which shall be used by Successful Respondent to perform the Services after the Commencement Date. Equipment Leases include those leases identified in **Attachment 2.2 Financial Responsibility Matrix**, those as to which the costs are included in the Financial Base Case, and those as to which Successful Respondent received reasonable notice and/or reasonable access prior to the Commencement Date. Equipment Leases also include all such leasing arrangements entered into by or for DIR, DCS Customers, any DIR Contractor, or Service Component Provider (SCP) during the Term. |
| Escrow Agreement | Has the meaning given in **MSA, Attachment 3 Form of Source Code Escrow**. |
| Event of Loss | Has the meaning given in **MSA, Attachment 2 Insurance and Risk of Loss**. |
| Expected Service Level | Means the desired level of performance for a Critical Service Level or Key Measurement, as set forth in **Attachment 1.3, Service Level Definitions and Performance Analytics**. |
| Expiration Date | Means the ending date of the Term as used in **MSA, Section 3.2 Extension**. |
| Extraordinary Event | A circumstance in which an event or discrete set of events has occurred or is planned with respect to the operations of DIR or the DCS Customers that results or shall result in a change in the scope, nature or volume of the Services that DIR or the DCS Customers shall require from Successful Respondent. Examples of the kinds of events that might cause such substantial increases or decreases include the following: (1) changes in locations where the DCS Customers operate; (2) changes in constituencies served by, or activities or operations of, the DCS Customers; (3) privatizations, dispositions, or reorganizations of the DCS Customers; (4) changes in the method of service delivery; (5) changes in the applicable regulatory environment or applicable Laws; and, (6) changes in DIR's or a DCS Customer's policy, technology or processes. |
| ETL | Extract, Transform, and Load. |
| FAQ(s) | Frequently Asked Question(s). |
| Federal Tax Information (FTI) | Any Federal tax information, including without limitation, and tax return-derived information received from the IRS. |
| FERPA | Family Educational Rights and Privacy Act. |
| FTE | Full Time Equivalent. |
| FTI | Federal Tax Information. |

| Term | Definition |
|---|---|
| Full Time Equivalent (FTE) | A level of effort, excluding vacation, holidays, training, administrative and other non-productive time (but including a reasonable amount of additional work outside normal business hours), equivalent to that which would be provided by one (1) person working full time for one (1) year. Unless otherwise agreed, one (1) FTE is assumed to be 1,920 productive hours per year. Without DIR's prior written approval, one (1) dedicated individual's total work effort cannot amount to more than one (1) FTE. |
| Fully Managed Services | Fully Managed Services mean that DIR and its vendor partners work together to provide all the hardware, software, tools, and staff to fully support IT infrastructure. |
| Governance Model | Has the meaning given in Article 8 DCS Governance Model. |
| Hardware Service Charge (HSC) | Has the meaning given in **Exhibit 2 Financial Provisions and Pricing, Section 2.3**. |
| Help Desk | The facilities, associated technologies, and fully trained DCS Customer staff who respond to calls, coordinate all problem and request management activities, and act as a single point of contact for end users. |
| HIPAA | Health Insurance Portability and Accountability Act. |
| Historically Underutilized Business(es) | The meaning given to such term by the Texas Comptroller of Public Accounts. |
| HSC | See Hardware Services Charge. |
| HUB | Historically Underutilized Business. |
| I/P/C | Incident, Problem, and Change. |
| IaaS | Infrastructure as a Service. |
| IIRIRA | Has the meaning given in **MSA, Section 8.7 Certifications**. |
| Incident | An event which is not part of the standard operation of a Service and which causes or may cause disruption to or a reduction in the quality of Services and DIR and/or DCS Customer productivity. |
| Income Tax | Any tax on or measured by the net income of a Party (including taxes on capital, net worth or revenue that are imposed as an alternative to a tax based on net or gross income), or taxes which are of the nature of excess profits tax, minimum tax on tax preferences, alternative minimum tax, accumulated earnings tax, personal holding company tax, capital gains tax, or franchise tax for the privilege of doing business. |
| Incumbent Personnel | Employees of the Incumbent SCP(s) or their subcontractors providing Services to DIR pursuant to the terms of an MSA by and between DIR and the Incumbent SCP(s). |
| Incumbent Provider(s) or Incumbent Service Component Provider(s) | The vendor or their subcontractors providing Services to DIR pursuant to the terms of the MSA by and between DIR and the vendor. Generally speaking, the Incumbent Service Component Provider for DCS is Atos. |
| Information Technology Infrastructure Library (ITIL) | A world-wide recognized best-practice framework for the management and delivery of IT services throughout their full lifecycle. The primary structure of the requirements in the Statements of Work are based on an ITIL v2 Foundations with ITIL v3 guidance in select functional areas (e.g., Request Management and Fulfillment) with the expectation of migrating towards ITIL v3 progressively as process improvements are incorporated into the Service Management Manual. |

| Term | Definition |
|---|---|
| Infrastructure | The entire portfolio of Equipment, System Software, and Network components required for the integrated provision and operation of DIR and DCS Customer's IT Systems and Applications. |
| In-Scope | Those Services or resources that are the subject of Successful Respondent's obligations under the Agreement. |
| IRS | Internal Revenue Service. A division of the U.S. Treasury Department responsible for collecting taxes. |
| ITIL | See Information Technology Infrastructure Library. |
| ITSCM | IT Service Continuity Management. Aims to manage risks that could impact IT services. |
| ITSM | Information Technology Service Management. Describes a strategic approach to design, deliver, manage, and improve the use of IT. |
| Key Personnel | Has the meaning given in Article 5 Successful Respondent Personnel Requirements. |
| KSL | Key Service Level. |
| Laws | All federal, state and local laws, statutes, ordinances, regulations, rules, executive orders, circulars, opinions, interpretive letters and other official releases of or by any government, or any authority, department or agency thereof. |
| Legacy Modernization Guide | The guide created by DIR to provide guidelines, principles, best practices and references for developing a plan to modernize a legacy environment. At the time of the Effective Date, the guide is located at this location: https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Legacy%20Modernization%20Guide.pdf |
| Level 1 Support | Support that is provided as the entry point for inquiries or problem reports from Authorized Users. If Level 1 personnel cannot resolve the inquiry or problem, the inquiry or problem is directed to the appropriate Level 2 personnel or a Third Party for resolution. |
| Level 2 Support | Support that serves as a consolidation point for inquiries and problems. For example, Level 2 Support might exist in a computer operation or a distribution/mail out center. If Level 2 personnel cannot resolve the inquiry or problem, the inquiry or problem is directed to the appropriate personnel or a Third Party for resolution. |
| Local Time | Central Standard Time or daylight savings time, as is then prevailing, in Austin, Texas. |
| Logical Security | Controlling access to information, software, and data by utilizing Operating Software parameters and Applications-level security controls. Logical Security includes logical separation of processors and disk and segregation of reusable storage media. |
| Losses | All losses, liabilities, damages (including punitive and exemplary damages), fines, penalties, settlements, judgments, interest and claims (including taxes), in each case that a court finally awards to a third party or which are otherwise included in the amount payable to a third party and all related costs and expenses (including reasonable legal fees and disbursements and costs of investigation, litigation, experts, settlement, judgment, interest and penalties), as incurred. |
| Mainframe Service Component Provider | The DCS SCP who has entered into a contract with DIR for the Mainframe Statement of Work. One (1) of eight (8) Service Components comprising the DCS Program within STS. |
| Major Incident | The highest category of impact for an Incident. A Major Incident results in significant disruption to business operations. |

| Term | Definition |
|---|---|
| Management Tools | All items used by Successful Respondent to deliver and manage the Services, including but not limited to software products and tools, code, scripts, bots, automation, and any and all methods, processes, inventions, machines, compositions, know-how, and show-how related thereto (and all modifications, replacements, Upgrades, improvements, enhancements, documentation, materials and media related thereto). Management Tools shall include all such products and tools in use or required to be used as of the Commencement Date, including those set forth in **Attachment 1.3 Service Level Definitions and Performance Analytics**, those as to which the license, maintenance, or support costs are included in the Financial Base Case, and those as to which Successful Respondent received reasonable notice and/or access prior to the Commencement Date. Management Tools also shall include all such products and tools selected and/or developed by or for DIR, any DCS Customer or Successful Respondent during the Term. |
| Marketplace | A type of e-commerce site where product or service information is provided by multiple third parties, whereas transactions are processed by the marketplace operator. |
| Materials | All tangible and intangible items and property, including but not limited to code; tools; scripts; bots; automation formulae; algorithms; processes; process improvements; procedures; designs; concepts; inventions; machines; articles of manufacture; compositions; improvements; methodologies; trade secrets; technology; Software (in both object and source code form); databases; specifications; configurations; any all methods, process, inventions, machines, compositions, know-how, and show-how related thereto; and all records thereof, including documentation, design documents and analyses, interface documentation, studies, tools, plans, models, flow charts, reports and drawings. |
| MDS | Master Data Services. A Master Data Management product from Microsoft that ships as a part of the Microsoft SQL Server relational database management system. Master Data Services is the SQL Server solution for master data management. |
| MDSS or SDS or MSDS | Material Data Safety Sheet, or a Safety Data Sheet, or a Material Safety Data Sheet. A document that lists information relating to occupational safety and health for the use of various substances and products. |
| Measurement Window | The time during, or frequency by, which a Service Level shall be measured. The Measurement Window will exclude approved scheduled maintenance. |
| Middleware | Software that facilitates interactions and integration between and among two (2) or more separate Software programs, Systems, or platforms. |
| MIM | Major Incident Management. The management of a Major Incident which demands a response beyond the routine incident management process. |
| Minimum Service Level | The minimum level of performance set forth **in Exhibit 1 SOW, Attachment 1.2 Service Level Matrix** with respect to each Service Level. |
| MIRT | Major Incident Response Team. |
| Monthly Charges | The total Charges invoiced by Successful Respondent in any calendar month for Services (excluding Pass-Through Expenses, Out-of-Pocket Expenses and Service Taxes). See **Exhibit 2 Financial Provisions and Pricing, Section 3.2**. |
| Monthly Invoice | Has the meaning given in **Exhibit 2 Financial Provisions and Pricing, Section 2.2.1.1**. |

| Term | Definition |
|---|---|
| Monthly Productive Hours Worked | With respect to any month and any Successful Respondent Personnel, the number of productive hours worked by such Successful Respondent Personnel, excluding non-productive time (e.g., commuting time, vacation, holidays, training unrelated to the Services, education, marketing, administrative staff meetings, medical leave, and military leave). |
| Multi-sourcing Services Integrator (MSI) | The Service Component Provider who has entered into a contract with DIR for Multi-sourcing Services Integrator services. |
| MSI Portal | A type of content management web site, password protected to allow secured access to and input of content as required in the Agreement. |
| Multi-Supplier Environment | Has the meaning given in Section 9.2 Multi-sourcing Services Integration and Cooperation. |
| New Services | Services requested by DIR, DCS Customers, or required by applicable Laws (without limiting the obligation of the Parties under **MSA, Section 8.11 Compliance with Laws**) (i) that are materially different from the Services, (ii) that require materially different levels of effort or resources from Successful Respondent to provide the Services, and (iii) which are not required for Successful Respondent to meet the Service Levels. For the avoidance of doubt, New Services shall not include (a) increases in the volume of Services for which there is an associated Resource Baseline or charging methodology, or (b) the disaggregation of an existing service from a Functional Service Area. |
| NIST | National Institute of Standards and Technology. |
| Noncompliance | Each instance that the Software, Equipment, Systems, or other Deliverable or milestone fails to meet its Acceptance Criteria or is otherwise deficient in DIR's reasonable discretion (in accordance with the SMM or other criteria agreed by the Parties, to the extent applicable). |
| Non-consolidated Compute | Includes service locations outside of the DIR CDCs as well as remote sites where break-fix services will also be performed. |
| Notice of Election | Has the meaning given in **MSA, Section 10.3.1 Notice**. |
| OEM | Original Equipment Manufacturer. |
| One-Time Charges | Any Charges that are specified by the Successful Respondent and which are non-recurring and are typically associated with start-up and implementation costs. |
| One-Time Deliverables | Those Deliverables that are non-recurring that have associated Deliverable Credits payable to DIR in the event Successful Respondent fails to successfully and timely complete such Deliverables. |
| Operating Level Agreements (OLA) | Has the meaning given in **MSA, Section 4.1 Overview**. |
| OS | Operating System. |
| Outage | A condition such that a System, Service, Application System, Equipment or network component is not Available or is substantially not Available and is impacting normal business operations. |

| Term | Definition |
|---|---|
| Out-of-Pocket Expenses | Reasonable, demonstrable and actual expenses due and payable to a Third Party by Successful Respondent that are approved in advance by DIR and for which Successful Respondent is entitled to be reimbursed by DIR under the Agreement. Out-of-Pocket Expenses shall not include Successful Respondent's overhead costs (or allocations thereof), general and/or administrative expenses or other markups. Out-of-Pocket Expenses shall be calculated at Successful Respondent's actual incremental expense and shall be net of all rebates and allowances. |
| Party(ies) | Has the meaning given in the recitals to the Agreement. |
| Pass-Through Expense(s) | The Successful Respondent expenses identified in **Exhibit 2 Financial Provisions and Pricing, Section 3.7** which DIR has agreed to pay directly or reimburse to Successful Respondent on an Out-of-Pocket Expenses basis. |
| Payment Deliverables | Those Deliverables that have associated payments due to the Successful Respondent after DIR approval of such Deliverables. Payment will be provided in accordance with the Agreement. |
| PCI DSS | Payment Card Industry Data Security Standard has the meaning given in **MSA, Section 6.5.4 Cardholder Data**. |
| PDU | Power Distribution Unit. |
| Penetration Tests | A type of Assessment that tests the vulnerability of Systems to unauthorized external interventions or improper uses. |
| Performance Category | A grouping of Critical Service Levels or Key Measurements. Critical Deliverables do not constitute a Performance Category. |
| PII | Personally Identifiable Information. Any data that could potentially identify a specific individual. |
| Plan | Has the meaning given in **MSA, Section 6.3.** |
| Portal | The online Internet site providing access and links to Services and other applications. |
| PPM | Project and Program Management. |
| Privacy Laws | Laws relating to data privacy or data protection. |
| Privileged Access | Any accounts that have escalated or administrative privileges. The ability to make back end, network, or OS configuration changes. Example account types: Root, DBA, Administrator. |
| Problem | An underlying cause of one (1) or more Incidents. A Problem is labeled a “Known Error” when the root cause is known and a temporary workaround or permanent solution has been identified. |
| Problem Management | The process of tracking and managing all problems arising in DIR and DCS Customer's IT environment, and resolving those problems arising from or related to the Services. |
| Production or Production Environment | The system environment in which an organization's data processing is accomplished. This environment contains DCS Customers’ business data and has the highest level of security and availability of all environments (includes training and other Production-like environments). |
| Project Manager (Successful Respondent’s) | The person or the person’s designee identified by the Successful Respondent as the responsible individual from the Successful Respondent’s organization to manage the project. |
| Project Milestone(s) | In accordance with Section 10.2 Deliverables, milestones produced and delivered as part of a Request for Service process and are specific to a project being delivered. DIR or DCS Customers shall have the right to review and accept or reject the milestones in accordance with the SMM. |

| Term | Definition |
|---|---|
| Project(s) | Means discrete units of work approved by DIR, undertaken to create a unique product or result. |
| Proposal | Has the meaning given in the preamble to the Agreement. |
| Protected Health Information (PHI) | Has the meaning given in **MSA, Section 6.3 DIR Personal Data**. |
| Public Cloud | Computing services offered by third-party providers where scalable and elastic capabilities are provided as a service to customers using Internet technologies. |
| Public Information Act | Has the meaning given in **MSA, Section 6.1.2 Disclosure of Confidential Information**. |
| QAT | Quality Assurance Team has the meaning set forth in Section 9.8.15 Project Management. |
| Quality Assurance (QA) | The actions, planned and performed, to provide confidence that all processes, Systems, Equipment, Software, and components that influence the quality of the Services are working as expected individually and collectively. |
| RAS | Remote Access Server. |
| Recovery Point Objective (RPO) | Recovery Point Objectives, as designated in Section 9.8.13 IT Service Continuity Management Requirements, expressed as the acceptable amount of data loss measured in time prior to an event that has been declared as a disaster. |
| Recovery Time Objective (RTO) | Recovery Time Objectives, as designated in Section 9.8.13 IT Service Continuity Management Requirements, expressed as the duration of time within which an Application, including all technology components included in the DCS Customer DR Plan must be recovered, restored and operational starting from the time of declaration of a disaster. |
| Recurring Deliverables | Those Deliverables to be provided on a scheduled and recurring basis that have associated Deliverable Credits payable to DIR in the event Successful Respondent fails to successfully and timely complete such Deliverables. |
| Refresh | The upgrading and/or replacing of Equipment and Software during the Term. |
| Reports | Has the meaning given in Section 6.4.1 Data and Reports. |
| Request Management | The process of tracking and managing all requests from Authorized Users arising in DIR's and DCS Customers' IT environment, and resolving those requests arising from or related to the Services. |

| Term | Definition |
|---|---|
| Required Consent(s) | The consents (if any) required to be obtained:<br>1. to assign or transfer to Successful Respondent DIR licensed Third Party Materials, Third Party Contracts, Equipment Leases or Acquired Assets (including related warranties).<br>2. to grant Successful Respondent the right to use and/or access the DIR licensed Third Party Materials, Third Party Contracts, and DIR Provided Equipment in connection with providing the Services.<br>3. to grant DIR, the DCS Customers and/or their designee(s) the right to use and/or access the Successful Respondent Owned Materials, Third Party Materials and Equipment acquired, operated, supported, used, or required to be used by Successful Respondent in connection with providing the Services.<br>4. to assign or transfer to DIR, the DCS Customers and/or their designee(s) any Developed Materials to the extent provided in the Agreement.<br>5. to assign or transfer to DIR, the DCS Customers and/or their designee(s) Successful Respondent Owned Materials, Third Party Materials, Third Party Contracts, Equipment leases or other rights following the Term to the extent provided in the Agreement.<br>6. all other consents required from third parties in connection with Successful Respondent's provision of, and DIR's and the DCS Customers' receipt and use of, the Services and Successful Respondent's performance of its obligations hereunder. |
| Resolution Time | The amount of time between the Start Time for an Incident and the time such Incident is Resolved. |
| Resolve or Resolution | The restoration of full Service or the completion of the Service Request in a manner acceptable to DIR or the applicable Authorized User in their reasonable discretion. Resolution may include the restoration of full Service by workaround or other alternative means. |
| Resource Unit (RU) | A measurable device, unit of consumption, or other unit or resource utilization associated with the Services, as described in **Exhibit 2 Pricing**, that is used for purposes of calculating Charges. |
| Resource Unit Category | A category of Resource Units which are measured and with respect to which charging rates or other charging mechanisms apply. |
| Respondent | A firm, company, entity or individual that responds to the solicitation. Unless the Contract clearly indicates otherwise, all terms and conditions of the Contract that refer to Respondent apply with equal force to Successful Respondent. |
| Response | Has the meaning given in the recitals of the Agreement. |
| Response Time | The elapsed time between the time one (1) event occurs such as when a call is placed or received and the time Successful Respondent responds to the event. |
| Retained Expense(s) | The expense types or amounts retained by DCS Customers as set out in **Exhibit 2 Financial Provisions and Pricing, Section 2.1.1.6**. |
| Retained Systems and Processes | Those systems and processes of DIR or a DCS Customer for which Successful Respondent has not assumed responsibility under the Agreement (including those provided, managed, operated, supported and/or used on their behalf by DIR Contractors). Retained Systems and Processes include equipment and software associated with such systems and processes. |
| RFO | Request for Offer. |
| RMAN | Recovery Manager. |

| Term | Definition |
|---|---|
| ROM | Rough Order of Magnitude. |
| Root Cause Analysis (RCA) | The formal process, specified in the SMM, to be used by Successful Respondent to diagnose the underlying cause of problems at the lowest reasonable level so that effective corrective action can be taken. |
| RPO | See Recovery Point Objective. |
| RTO | See Recovery Time Objective. |
| SAN | Storage Area Network. |
| SCP | Service Component Provider. |
| SDC | San Angelo Data Center. |
| Security | Means of safeguarding and controlling access to information, software, and data by utilizing policies, procedures and actions, including operating software parameters and applications-level security controls. Security includes logical separation of processors and disk and segregation of reusable storage media. |
| Security Assessment Company | Has the meaning given in Section 9.8.11.8 Security Assessments. |
| Security Plan | Has the meaning given in Section 9.8.11 Information Security Management Requirements. |
| Security Program | Has the meaning given in Section 9.8.11.88 Security Assessments. |
| Security Software | Has the meaning given in **Exhibit 2 Financial Provisions and Pricing, Attachment 2.2 Financial Responsibility Matrix, Network Tab**. |
| Server | Any computer that provides shared processing or resources (e.g., Application processing, database, mail, proxy, firewalls, backup capabilities, print, and fax services) to Authorized Users or other computers over the Network. A Server includes associated peripherals (e.g., local storage devices, attachments to centralized storage, monitor, keyboard, pointing device, tape drives, and external disk arrays) and is identified by a unique manufacturer's serial number. |
| Service(s) | Has the meaning given in **MSA, Article 4 Services**. |
| Service Component | A single area which is represented with a Statement of Work (SOW) (i.e., Texas Private Cloud, Managed DCS Network, Security Operations Services, etc.). |
| Service Component Providers (SCPs) | Means, collectively, all Service Component Providers, excluding the MSI, who have entered into an agreement with DIR to provide the services required by one (1) or more Service Component Statement(s) of Work. |
| Service Delivery Failure | Has the meaning given in Section 6.9 Service Level Improvement Plans. |
| Service Desk | The facilities, associated technologies, and fully trained staff who respond to Calls, facilitate all Incident Management, Problem Management, Change and Request Management activities, and act as a single point of contact for coordination and communication to Authorized Users and SCPs in regard to the Services. |
| Service Level(s) | Individually and collectively, the quantitative performance standards for the Services set forth in **Attachment 1.2 Service Level Matrix** and in **Attachment 1.3 Service Level Definitions** of the Agreement. |
| Service Level Credit Allocation Percentage | The percentage of the Allocation of Pool Percentage allocated to a Critical Service Level within a Performance Category. |
| Service Level Credit Start Date | The period beginning ninety (90) days after the Commencement Date wherein Successful Respondent will be liable for Service Level Credit(s) or CAP Failure Credit(s). |

| Term | Definition |
|---|---|
| Service Level Credits | The monetary amounts that the Successful Respondent shall be obligated to pay to DIR (or apply against Monthly Charges) in the event of Service Level Defaults. |
| Service Level Default | Occurs when a Minimum Service Level has not been met. |
| Service Level Invoice Amount | Charges due and owing for the preceding month, including the Monthly Base Charge and any additional Charges, including, to the extent applicable, any other amounts payable by DIR to Successful Respondent pursuant to the express terms of the Agreement (excluding payments for Transition Milestones Transformation Milestones, and HSC/SSC Charges). |
| Service Management Manual (SMM) | The management procedures manual for the Services as described in **Exhibit 1 SOW, Attachment 1.4 SMM Content and Organization**. |
| Service Request (or Request for Service) | A request for information, advice, access, or standard change to an IT service that does not require solution proposal development. Examples of such Service Request include provisioning ID access, password resets, and Service Catalog requests. |
| Service Taxes | All sales, use, excise, and other similar taxes that are assessed against either Party on the provision of the Services as a whole, or on any particular Service received by DIR or the DCS Customers from SCPs, excluding Income Taxes. |
| Severity Level | The categorization of a problem associated with the Services based on the potential impact of the problem to DIR and any DCS Customer, as further defined in **Attachment 1.3 Service Level Definitions and Performance Analytics, Section 1.1**. |
| SLAs | Service Level Agreements. |
| SMM | Service Management Manual. |
| Software | All Materials consisting of software programs and programming (and all modifications, replacements, Upgrades, enhancements, documentation, materials and media related thereto), including Antivirus Software, Application Software, Development Tools, and System Software. |
| Software Service Charge (SSC) | Has the meaning given in **Exhibit 2 Financial Provisions and Pricing, Section 2.3**. |
| Solution Request or Request for Solution | A Service Request that requires development of a proposal for DCS Customer approval to fulfill the request. |
| SOW | Statement of Work. |
| Specialized Services | Has the meaning given in **MSA, Section 4.10 Access to Specialized Successful Respondent Skills and Resources**. |
| Specifications | Means, with respect to processes, Software, Equipment, Systems or other contract deliverables to be designed, developed, delivered, integrated, installed, and/or tested by Successful Respondent, the technical, design and/or functional specifications set forth in Third Party Vendor documentation, in a New Services or Project description requested and/or approved by DIR, or otherwise agreed upon in writing by the Parties. |
| SQL | Structure Query Language. |
| SRT | Schedules, Retentions, and Targets document. |
| SSA | Social Security Administration. |
| SSC | Software Service Charge. |
| SSMS | SQL Server Management Studio. |
| Staffing Plan | Has the meaning given in Section 2.5.9 Staffing Plan and Time Commitment. |
| Standard of Due Care | Then-current accepted industry best practices for network and data security that are employed by members of the Peer Group. |

| Term | Definition |
|---|---|
| Start Time | With respect to an Incident or a Call, the time when the Incident ticket is created. With respect to an Outage, the earlier of the time when the Incident is detected or should have been detected (by the applicable monitoring for the System). If more than one (1) ticket is created for the same root cause, the Start Time shall be based on the earliest of the ticket creation times. |
| State Data Center(s) | The State data center in San Angelo, Texas, or Austin, Texas. |
| State Legislature | The governmental legislative body of the State. |
| State or State of Texas | The State of Texas, unless expressly stated otherwise. |
| Statement(s) of Work (SOW) | Means this document, **Exhibit 1 SOW**, and its attachments and appendices. |
| Strategic Plans | The plans that may be periodically developed by DIR that set forth DIR's key operational objectives and requirements and outline its strategies for achieving such objectives and requirements. DIR may revise the Strategic Plan from time to time. The Strategic Plan is likely to include both annual and multi-year strategies, objectives, and requirements. |
| Subcontract | An agreement between the Successful Respondent and their Subcontractor(s). |
| Subcontractor(s) | Subcontractors (of any tier) of Successful Respondent, including Affiliates of Successful Respondent performing Services under the Agreement pursuant to **MSA, Section 4.12 Subcontractors**. |
| Successful Respondent | The Party to this Agreement. |
| Successful Respondent Personnel | Those employees, representatives, contractors, subcontractors, and agents of Successful Respondent and its Subcontractors. |
| System(s) | An interconnected grouping of manual or electronic processes, including Equipment, Software and associated attachments, features, accessories, peripherals and cabling, and all additions, modifications, substitutions, Upgrades or enhancements to such System. Systems include all Systems in use or required to be used as of the Commencement Date, all additions, modifications, substitutions, Upgrades, or enhancements to such Systems and all Systems installed or developed by or for DIR, the DCS Customers or Successful Respondent during the Term. |
| Technology Evolution | Any improvement, upgrade, addition, modification, replacement, or enhancement to the standards, policies, practices, processes, procedures, methods, controls, scripts, product information, technologies, architectures, standards, equipment, software, systems, tools, products, transport systems, interfaces and personnel skills available to provide the Services in line with the best practices of first tier leading providers of services that are the same as or similar to the Services. Technology Evolution includes, as relating to such items for such purpose: higher capacity, further scaling and commercializing of processes, more efficient and scalable processes, new versions and types of applications and systems/network software, new operational or IT Infrastructure processes, and new types of hardware and communications equipment that shall enable Successful Respondent to perform the Services more efficiently and effectively as well as enable DIR and the DCS Customers to meet and support their operational requirements and strategies. |
| Technology Plan | Has the meaning given in Section 4.2 Technology Planning and Optimization Roadmap. |
| Technology Solution Services | The Services detailed in this Agreement. |

| Term | Definition |
|---|---|
| Term | The Initial Term and the Renewal Terms, if any, including any period during which Termination Assistance Services are provided by Successful Respondent under the Agreement. |
| Termination Assistance Services | (i) The Services (including the terminated, insourced, resourced or expired Services, the Services described in **MSA, Section 7.6** of the Agreement and throughout Article 11 of this SOW and, in each case, any replacements thereof or supplements thereto), to the extent DIR requests such Services during a Termination Assistance Services period; (ii) Successful Respondent's cooperation with DIR, DCS Customers and their designee(s) in the orderly transfer of the Services (or replacement or supplemental services) to DIR, the DCS Customers and/or their designee(s); and (iii) any New Services requested by DIR in order to facilitate the transfer of the Services (or replacement or supplemental services) to DIR, the DCS Customers and/or their designee(s). |
| Termination Charge | The termination charges payable by DIR as set forth in **MSA, Section 13.10.2 Termination Charges**. The Termination Charge shall be calculated as of the later of (i) the end of the Term (or the date of termination of the applicable Services under the Agreement), and (ii) the satisfactory completion of all Termination Assistance Services. |
| Texas Data Centers Services (or Data Center Services, DCS) | A program administered by DIR providing Compute and Print/Mail services to eligible DCS Customers. |
| Third Party Contract(s) | All agreements between Third Parties and DIR, any DCS Customer, or Successful Respondent that have been or shall be used to provide the Services. |
| Third Party Materials | Materials that are owned by Third Parties and provided under license or lease to Successful Respondent, DIR or any DCS Customer and that have been or shall be used to provide or receive the Services. Third Party Materials shall include Materials owned by Subcontractors (excluding Affiliates of Successful Respondent) and used in the performance of the Services. |
| Third Party Vendor(s) | A Third Party that provides products or services to any Party that is related to, or is in support of, the Services (e.g., hardware vendors, premier support contracts, etc.). Third Party Vendors do not include Subcontractors. |
| Third Party(ies) | A legal entity, company, or person(s) that is not a Party to the Agreement and is not an Affiliate of a Party. |
| Time-critical (regarding Deliverables) | Deliverables with an expedited review period of five (5) Business Days, designated with a "T". This is further detailed in Sections 10.2 Deliverables, 10.6 Acceptance Review Period, and 10.7 Noncompliance. |
| TQM | Total Quality Management. |
| TR&R | Technology Refresh and Replenishment. |
| Transformation Services | The consolidation activities, functions and deliverables, and the implementation of the technology and other process changes, described in the transformation plan. |
| Transition | Includes all transition activities and deliverables to be completed and provided by Successful Respondent in connection with the migration to Successful Respondent's Services, and the dates by which each is to be completed by Successful Respondent as further defined in Article 2 Transition Services. |
| Transition and Transformation Charges | Has the meaning given in **Attachment 2.1 Pricing and Volumes**. |

| Term | Definition |
|---|---|
| Transition Milestones | Has the meaning given in **Exhibit 2 Financial Provisions and Pricing, Section 3.5.2** . |
| Transition Plan (also Transition Project Plan) | The plan set forth in Section 2.5 Transition Project Plan and developed and updated pursuant to Section 2.5.2 Transition Project Plan Critical Deliverable, which identifies all material transition activities and deliverables to be completed and provided by Successful Respondent in connection with the migration to Successful Respondent of the Services, and the dates by which each is to be completed by Successful Respondent. |
| Transition Services | The transition activities, functions and deliverables described in the Transition Plan and such other tasks as are necessary to enable Successful Respondent to provide the Services. |
| Transport | A commercial service providing the carriage or transmission of voice, video, or data electronic impulses over a distance. |
| TRG | Technical Recovery Guide. |
| TSG | Technology Solutions Group. |
| TSLAC | Texas State Library and Archives Commission. |
| TSM | Tivoli Service Manager. |
| TSS | Technology Solution Services. |
| Type R Service Levels | Type R Service Levels are related measures shared between the MSI and the SCP(s) as defined in Section 6.3 Shared and Related Service Levels and Types. |
| Type U Service Levels | Type U Service Levels are intended to measure Services that are specific to one (1) DCS SCP's performance, and therefore are not shared between DCS SCPs as defined in Section 6.3 Shared and Related Service Levels and Types. |
| Unanticipated Change | A material change in the technologies and/or processes available to provide all or any portion of the Services which is outside the normal evolution of technology experienced by the Services, that was not generally available as of the Effective Date and that would materially reduce Successful Respondent's cost of providing the Services. |
| Upgrade(s) | Updates, patch installations, modifications, renovations, refreshes, enhancements, additions, substitutions and/or new versions or releases of Software or Equipment. For purposes hereof, a workaround or fix to Software or Equipment also constitutes an Upgrade. |
| UPS | Uninterruptable Power Supply. |
| Use | To load, access, execute, use, manipulate, practice, process, make, have made, operate, copy, execute, compile, store, purge, reproduce, display, perform, distribute, transmit, receive, modify, maintain, enhance, upgrade, store, create Derivative Works, and exercise any other similar rights; provided however that with respect to Third Party Materials that are Software, unless otherwise permitted under the applicable license agreement, the term "Use" shall not include the right to modify or create Derivative Works. |
| Virtual Data Center (VDC) | Means a logical environment representing a dedicated networking and security configuration for a specific DCS Customer. |
| VLANs | Virtual Local Area Networks. |
| VPN | Virtual Private Network. |
| WBS | Work Breakdown Structure. |
| Wide Area Network (WAN) | A long-haul, high-speed backbone transmission Network, consisting of WAN Equipment, Software, Transport Systems, Interconnect Devices, and Cabling that, and other services as they become available that are used to create, connect, and transmit data, voice and video signals, between or among: (i) LANs, and (ii) other locations that do business with the State and for which DIR is responsible for allowing Connectivity. |

| Term | Definition |
|---|---|
| Work Order | Has the meaning given in the Agreement. |
| Work Product | (i) All reports and manuals, including Transition Plans, Transformation Plans, business requirements documents, design documents, manuals, training and knowledge transfer materials and documentation, (ii) the Service Management Manual, (iii) Desktop Procedures, and (iv) any literary works and other works of authorship created under the Agreement that express, embody or execute or perform a function, method or process that is specific to the business of DIR or DCS Customers. Work Product includes customized reports, manuals and forms, but not the original unmodified versions used by Successful Respondent as a starting point for creating the customized version. |

**NOTE:** Definitions in this table are applicable to all Exhibits and Attachments making up the Security Operations Services Request for Offer (RFO) and subsequent Contract. Pricing-specific definitions are found in **Exhibit 2 Pricing** documents.

# 1. Business Background and Objectives

## 1.1. Background and Introduction

(a) Texas Data Center Services (DCS) data centers and the State's underlying telecommunications infrastructure provide a central hub for participating DCS Customers as they carry out their missions. Increasing use of the DCS program's cloud offerings (Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) providers) provide even more options for DCS Customers.

(b) Security is currently embedded in services provided by the DCS Service Component Providers (SCPs) and governed by the Multi-sourcing Services Integrator (MSI) and the Texas Department of Information Resources (DIR). Through this Request for Offer (RFO), DIR seeks to centralize many of the security services, establishing a focused structure that manages and operates security functions relative to the scope of this RFO.

(c) The primary goals of the DCS Security Operations Services include:

- (i) Driving a proactive approach to security and protecting DCS infrastructure, network, systems and applications;
- (ii) Providing real-time threat detection, situational awareness, threat defense, and actionable intelligence;
- (iii) Reducing the risk to DCS Customers and SCPs by implementing a holistic approach to security, including governance and enablement of services extensible to all SCPs, DCS infrastructure elements, and DCS networks;
- (iv) Collecting enterprise baseline metrics to understand what is normal and what is an anomaly;
- (v) Improving coordination and communication to all involved parties when a cybersecurity event is underway and to bring all tools and resources to bear on the event;
- (vi) Ensuring DCS Security governance and compliance processes and tools are applied and deployed in the most effective, efficient, repeatable and scalable manner to provide a maximal level of defense against inappropriate access to DCS assets;
- (vii) Coordinating with DIR and STS governance processes to establish and maintain Security policies and standards applicable to delivery of services to customers across all SCPs;
- (viii) Providing security monitoring aggregation across all services;
- (ix) Utilizing tools, methods, and Successful Respondent expertise to conduct security operations and oversee response and remediation activities between DCS SCPs, networks, and infrastructure segments and domains;
- (x) Establishing coordination between DCS Customers, DIR, MSI, TSS, and DCS SCPs to defend and respond against attacks and remediate and mitigate risks;
- (xi) Define standards for hardening infrastructure and procedures against exposures by minimizing manual methods, eliminating inconsistencies, and encouraging automation; and
- (xii) Implementing a standard, repeatable, and proactive approach to security within DCS.

(d) DCS is the central, consolidated computing and networking hub for DCS Customers. As such, DIR plans to develop a centralized process for consolidating, monitoring, and coordinating the management of DCS security operations under a central point of accountability that leverages the robust standards, processes, procedures, and tools providing total oversight over all DCS provided services – private/public compute, print/mail, mainframe, storage, technology solution services, LAN network and WAN networks.

(e) This Service is an essential "first step" in determining the feasibility and merits of a statewide security approach. However, Respondents should specifically limit their response to the scope, activities, and deliverables outlined herein (i.e., DCS Customers, DIR, MSI, and DCS SCPs).

(f) **NOTE**: Many DCS Customers maintain their own security capabilities that are out of scope for this RFO. Several large agencies maintain security operations centers that are responsible for the monitoring, management, and maintenance of security elements within their environments.

## 1.2. Statewide Portal for Enterprise Cybersecurity Threat, Risk and Incident Management (SPECTRIM) System

DIR deployed a governance, risk and compliance tool called SPECTRIM for security incident reporting. The tool platform is Archer's RSA product. DIR is responsible for purchasing and maintaining the tool. The Office of the Chief Information Security Officer (OCISO) retains responsibility for SPECTRIM configurations, policies and procedures; however DIR intends the Successful Respondent will be onboarded as "users" of the system and, upon mutual determination of need, will be allowed to integrate data feeds, incidents, and alerts as part of a systems integration effort. Each party is responsible for updating their data in SPECTRIM. The OCISO uses the data in the system to track and report on trends (especially incidents). Other departments at DIR also use data from the system for their reports and analysis. All DCS SCPs have a responsibility to properly update the system with information on alerts, events, incidents, etc.

## 1.3. Service Objectives

(a) The Successful Respondent is responsible for the consolidation of security services including the associated management and operations for DCS Security Service Delivery Center described below.

(b) DIR seeks to establish a central point of security service operations responsibility with advance security and monitoring capabilities providing DCS Customers secure private and public cloud-based DCS services with vital defense protection against intrusion and inappropriate access to DCS environments.

(c) DIR seeks standardization and automation of DCS security capabilities via an end-to-end Service that includes services such as: DCS Customer engagement and onboarding; vulnerability remediation; automated provisioning of security templates; enablement of DCS security monitoring and operational tools; active security monitoring; and remediation assistance.

(d) DIR seeks a holistic security service solution to protect DCS infrastructure, systems, services, and data which is highly automated and scalable. The Successful Respondent will provide comprehensive security services at an enterprise level to:

    (i) Establish cybersecurity rules and controls, including:

A. Establish DCS security policies and standards.
B. Provide DCS SCPs and DIR with cross boundary security control baselines and security information visibility to inform program planning.
C. Coordinate and consolidate security standards and stewardship for all DCS program areas and SCPs.
D. Deploy and operate a Privileged Access Management (PAM) solution to provide a common way to track privileged IDs for services provided by DCS and enable centralized monitoring and ID vulnerability analysis.
E. Establish and operate a vulnerability management program to identify vulnerabilities by analyzing defined SCP-level scans, initiating mitigating actions and ensuring they are followed through to closure.

(ii) Identify and lead the mitigation of cybersecurity issues, including:
A. Operate Security Incident and Event Monitoring (SIEM) capabilities to aggregate enterprise-level security logs and perform cross-tower correlations for DCS services.
B. Operate Security Operations Center (SOC) function to perform reactive and proactive cybersecurity threat analysis across DCS services.
C. Lead security incident responses to closure.

(iii) Instrument and automate security operations, monitoring, operational controls and hardening activities.

(iv) Ensure security elements are provisioned and managed utilizing software-defined methods and capabilities eliminating manual efforts and to promote a "secure-first-time" deployment model that is highly standardized and repeatable.

(v) Enable other DCS SCP operators as "trusted peers" to promote DCS Customer flexibility of deploying Private and Public Cloud hybrid solutions which are safe, hardened, and trusted without concerns of security limitations or nuances.

### 1.3.1. Service Differentiators and Required Outcomes

(a) Security across multi-Customer, multi-provider, centralized computing assets, and the Public Cloud represents one (1) of the largest concerns in public sector computing. DIR seeks a Respondent who can drive the required step-change in security capabilities for DCS inclusive of design, build, operate, maintain, secure, and monitoring activities.

(b) Respondent, via the Response, should propose a solution demonstrating how they will:

(i) Drive higher levels of security capabilities for DCS infrastructure while removing obstacles to agility, integration, delivery, and holistic security monitoring in the DCS environment;

(ii) Implementation of continual improvement that includes assessment of the DCS threatscape as new threats and security technologies are developed to counteract those threats; and

(iii) Establish security strategy for DCS assets that promotes consolidation and consistency of approach across all services provided by the DCS program achieving volume/scale efficiencies.

(c) DIR has identified several objectives that must apply to the DCS Security Service relationship going forward. Specifically:

**Table 2: Security Service Objectives**

| Objective Area | Key Service Requirements and Respondent Differentiators |
|---|---|
| Service Delivery | ▪ Continued robust service delivery model leveraging the framework outlined by the MSI, inclusive of tools, technology, and processes<br>▪ Leverage of modern tools, techniques and processes, both those introduced by the Successful Respondent and those implemented via the design of the MSI<br>▪ Automation of integration between Successful Respondent tools and technology and interfaced MSI and SCP tools and reporting mechanisms to allow for real-time analysis of Service components<br>▪ Defined roles and responsibilities with no gaps or non-complimentary overlaps<br>▪ Accountability and ownership by all parties and stakeholders |
| Delivery Team and Personnel | ▪ Aligned as business partner to the DCS SCPs and MSI as opposed to "vendor"<br>▪ Seek challenges and serve DCS Customers through the SCPs and MSI by going the extra distance<br>▪ Integrated with MSI and DCS SCPs<br>▪ Fluent and viewed as experts in their respective disciplines and work as a cohesive team with SCPs and DCS Customers as needed as opposed to "operational silos"<br>▪ Commitment to continual evolutions and upgrades to the skill composition of the team to keep pace with technological change, Texas IT direction, preferences, and standards as they evolve over the duration of the Contract<br>▪ Provide and participate in ongoing education, training, and certifications, as appropriate |
| Operational Reliability and Discipline | ▪ Alignment with the MSI processes and tools<br>▪ Robust planning, design, build, test, implement, and release processes<br>▪ Robust change and communications management<br>▪ Reliable, repeatable, and robust execution that results in consistent operational quality<br>▪ Tool- and process-centric enablement of operations, within the Service and in collaboration with the toolsets offered by the MSI and Security<br>▪ In collaboration with the MSI and DIR, management of the full-service lifecycle<br>▪ Continuous Security Improvement (CSI) and Total Quality Management (TQM), which implies measurable performance indicators in compliance with Service Level Agreements (SLAs) |
| Delivery Culture | ▪ Collaborative, collegial, transparent, and integrated with DCS Customer operations and application development teams<br>▪ Focused on SCPs, MSI and DCS Customers' objectives and outcomes as opposed to meeting minimum requirements<br>▪ Strict adherence to time, quality, budget, and personal commitments<br>▪ DCS advocacy and evangelism, working with DIR and the MSI in DCS Customer adoption and legacy systems retirement<br>▪ Inclusion of DevSecOps into standard Service operations |

| Objective Area | Key Service Requirements and Respondent Differentiators |
|---|---|
| Change Management and Control | ▪ Integration with MSI platforms, technology and processes for standard ITIL-based service management functions consistent across all SCPs<br>▪ Changes to production (code, process, configuration, reports and otherwise) controlled with versioning, testing and verification<br>▪ Change management and environment changes supported by processes and tools<br>▪ High-touch communications and expectation management with DCS Customer service delivery and DIR stakeholder organizations |
| Security, Reliability, and Repeatability | ▪ Continue to operate in a secure and reliable environment that protects sensitive and personal information contained in the systems that operate on a DCS platform<br>▪ Continue to ensure operations are reliable and repeatable from a service quality and predictability perspective<br>▪ Meet or exceed SLAs while striving for continuous improvement<br>▪ Full compliance with and understanding of evolution of security and/or data privacy requirements– including, but not limited to: Criminal Justice Information Services (CJIS), Payment Card Industry (PCI), Personally Identifiable Information (PII), Federal Tax Information (FTI), Social Security Administration (SSA), etc. |
| Software Enabled Platform for Consolidation | ▪ Partner with TSS, MSI and SCPs in identifying consolidation opportunities for DCS Customer compute elements and consume network services that could better be served via an "enterprise approach"<br>▪ Act as a legacy modernization change advocate for DCS Customers |
| Cost Considerations | ▪ Improve DCS operational efficiencies while seeking to optimize delivery through automation and elimination of redundancy or non-value-added activities and elements<br>▪ Extending DCS capabilities by enabling DCS Customers to migrate infrastructure assets to virtual and cloud (private or public) assets |

## 1.4. DCS Security Operations Services Scope

The scope of DCS Security operations services includes: Security standards and operational security oversight of the DCS Private and Public Cloud environments (logical and physical elements) including:

(i) Compute services: IaaS, PaaS, SaaS including compute, storage and enabling technologies for Private Cloud services, Public Cloud Management and Public Cloud services;

(ii) Network services including:

A. Local Area Networks - within DCS data centers including Virtual Networks, i.e., VLANs/VPCs/VNETs;

B. Data Center WAN Network - connecting the DCS Consolidated Data Centers and DCS public cloud services;

C. Permanent Virtual Circuits;

D. Remote access - Virtual Private Networks, tokens, certificates, encryption keys, Remote Access Service (RAS) devices; and

E. Legacy and future state environments of all network devices and appliances supporting the DCS program (i.e., access switches, firewalls, Web Application Firewalls (WAFs), load balancers, network monitoring/management consoles, redundant network elements, wired/optical network elements and devices).

(iii) Excluding telecommunications services;

A. MSI infrastructure and services;
B. TSS coding practices and managed applications;
C. DCS print/mail digitization services; and
D. DCS mainframe services.

## 1.5. Organization of the Work Areas within this Exhibit and Across the RFO

### 1.5.1. DCS Security Services: Transition Services

(a) The Successful Respondent shall drive an orderly and well executed transition of in-scope security management services and operations of all systems, components, documentation and related operational support roles, transitioning from DIR's current DCS environment to the Services described in this SOW. Detailed requirements are contained in Article 2 Transition Services.

(b) There is currently office space for Successful Respondent staff available at the Austin and San Angelo Data Center. Respondents should indicate in their proposals whether and how many staff will be located at each data centers.

### 1.5.2. Transformation Services

(a) DIR has identified several transformational projects that, if successfully designed and implemented, will provide transformational services to both DCS Customers and underlying DCS SCPs. These projects must provide high quality, cost-effective service with standardized processes and procedures and leverage a focused Successful Respondent team that is fluent in modern development and multi-project portfolio skills.

(b) The Successful Respondent team must be experienced in solution delivery and utilize a repeatable, proven and disciplined methodology and preferably have worked on large/multi-vendor initiatives. The Successful Respondent's methodology will be the centerpiece of the solution delivery team and used to ensure project success and therefore must be proven to produce results in such projects.

(c) Generally, these projects range from large, multi-year initiatives to medium (e.g., approximately six (6) months) and small (e.g., three (3) months or less) rapid delivery cycles. The scope of the transformation competency is primarily focused on medium and small projects.

(d) DIR is seeking expertise and leadership in the identification, prioritization, analysis, design, development, testing, and deployment of high-value opportunities across technologies and lines of business as supported by the DCS program. Successful partnership in these opportunities will require proven methodologies, alignment with strategy and priorities, and depth of talent and expertise. The in-scope initiatives typically transcend technologies and stakeholder groups and require a significant degree of technical integration and coordination of project resources (DCS Customer and DCS SCPs).

(e) **NOTE**: Transformational projects are optional; the numbering of these projects is **purely for identifying purposes only**.

(f) DIR may instruct the Successful Respondent to complete these transformation projects in any order, in whole or in part, and at any time during the Contract or may elect not to undertake any of the

transformational projects listed herein. Detailed requirements are contained in Article 7 Transformation Projects.

#### 1.5.3. Steady State Operations and Security Services

(a) Steady state operations and Security services begins at Commencement, when transition activities are concluded, through Contract termination. The Successful Respondent will, through ongoing support and maintenance control processes, maintain support of the solutions developed by the Successful Respondent during the term of the Contract.

(b) Detailed requirements are contained in Article 3 Security: Steady State Run Services**.** The requirements in Article 3 are aimed at supporting the following seven (7) core functional areas.

(i) Security Policies and Standards

(ii) Privileged Access Management (PAM)
(iii) Vulnerability Management Program
(iv) Security Incident and Event Monitoring (SIEM)
(v) Active Threat Identification
(vi) Incident Response Command
(vii) Program Management and Operations

## 2. Transition Services

### 2.1. Operations Take Over

At Commencement, the Successful Respondent will either take over operations from the Incumbent Provider as they exist at that time or implement new services that meets or exceeds then-current capabilities. In other words, the Successful Respondent must have the skills and capabilities to perform security operations for the environment as it is described in the Article 1 Business Background and Objectives. The Transition Plan must articulate the Successful Respondent's approach and schedule to assume current operations as of Commencement as well as those impacted by any network or infrastructure changes proposed after Commencement.

### 2.2. General Transition Requirements

(a) The Successful Respondent will be responsible for the migration of supported networks, hardware and software, configuration information, system components, documentation, and related operational and security support roles in transitioning from the current Contract. The Successful Respondent's transition requirements include the tasks and activities described below.

(b) The Successful Respondent shall perform the Transition Services in accordance with the timetable set forth in the Transition Project Plan. Successful Respondent shall assist DIR in connection with DIR's and/or the DCS Customers' evaluation or testing of the deliverables set forth in the Transition Project Plan. Except as otherwise expressly stipulated in the Transition Project Plan (which will appropriately acknowledge that some element of disruption may occur as in any such transition, but shall in all events be minimized), Successful Respondent shall perform the Transition Services in a manner that shall not:

(i) disrupt or have an unnecessary adverse impact on the activities or operations of DIR or the DCS Customers,
(ii) degrade the Services then being received by DIR or the DCS Customers, or
(iii) disrupt or interfere with the ability of DIR or the DCS Customers to obtain the full benefit of the Services.

(c) Without limiting its obligations or responsibilities, prior to undertaking any transition activity, Successful Respondent shall discuss with DIR and the relevant DCS Customers all known DIR and DCS Customer-specific material risks and shall not proceed with such activity until DIR is satisfied with the plans with regard to such risks (provided that, neither Successful Respondent's disclosure of any such risks to DIR, nor DIR's acquiescence in Successful Respondent's plans, shall operate or be construed as limiting Successful Respondent's responsibility under this Agreement). Successful Respondent will participate in Transition meetings with the MSI and other DCS SCPs.

## 2.3. Knowledge Transfer

(a) During the period following the Effective Date and prior to the Commencement Date, Successful Respondent will use its best efforts to acquire the practical skill, knowledge and expertise from the personnel who are providing the Services prior to the Effective Date in relation to the delivery of the Services, including the knowledge necessary for the Successful Respondent to perform the Services. Successful Respondent will accomplish such knowledge transfer, as appropriate, by interviewing personnel currently performing the Services as well as reviewing information, records and documents related to the provision of the Services. The information to be reviewed to affect the obligations of such knowledge transfer includes:

(i) copies of procedures and operations manuals,
(ii) relevant system, software and/or hardware information;
(iii) a list of third-party suppliers of goods and services which are to be transferred to DIR or Successful Respondent;
(iv) key support contact details for third party supplier employees; and
(v) information regarding work in progress and associated unresolved faults in progress.

(b) Successful Respondent shall promptly (within one (1) DIR Business Day) notify DIR of any lack of cooperation or assistance on the part of any DCS Customer, DIR Contractor or any third party that impedes or hinders Successful Respondent's efforts to comply with this obligation.

(c) Transition work includes (at a high level):

(i) Conducting an orderly Transition;
(ii) Establishing all Service processes and responsibilities, including on-boarding of all Service Transition and Steady State Service personnel;
(iii) Implementing the entire Service inclusive of all DIR required processes, tools, data sharing, and reporting as required by DIR and within the MSI operating model;
(iv) Ensuring that the Service is performing to DIR requirements and the Successful Respondent is responsible for the Service in its totality with no requirements or obligations residing elsewhere; and
(v) Completing all required deliverables, milestones and quality standards.

## 2.4. Transition Management Requirements

(a) During the Transition period, the Successful Respondent will plan, prepare for, and conduct the migration of Service systems operations. Transition may include the migration of monitoring systems and related operational support from currently existing facilities, locations, and personnel to the Successful Respondent's provided equivalents.

(b) The Successful Respondent shall:

(i) Coordinate with DIR to schedule the installation of any required secure connectivity.
(ii) Implement processes and controls to prevent disruption of DCS Customers' business operations.
(iii) Meet with DIR and the MSI and provide updates as to the status of the work involved in Transition at a time and frequency as mutually agreed to in the Transition Project Plan and upon request by DIR or the MSI.
(iv) Ensure adequate staff are committed to the Transition services across workstreams, including but not limited to one or more dedicated Project Managers.
(v) Provide project management over all Successful Respondent Service Transition and SCP integration Transition.
(vi) Provide sufficient staff, tools and processes to ensure all Services successfully transition from the Incumbent SCP without service degradation to Customers.
(vii) Ensure other SCPs successfully transition to Successful Respondent's services by Commencement without service degradation to DCS Customers.
(viii) Develop a detailed Transition Plan including the Successful Respondent's approach to transitioning Services from the Incumbent Provider. The Transition Plan should include, at a minimum, all systems, processes, data (e.g., Incumbent ITSM data) and reporting that is required to transition from the Incumbent Service Provider.
(ix) Be responsible for all knowledge transfer from the Incumbent Provider.
(x) Provide routine reports and communication on Transition status to DIR, MSI and SCPs, as directed by DIR.
(xi) Meet with DIR, MSI and SCPs to report on Transition activities, status, issues and risks.
(xii) Resolve issues collaboratively with DIR, MSI and SCPs to meet Transition schedule.
(xiii) Communicate the status of Transition, training, and changes to DIR.
(xiv) Identify all integration points of the Successful Respondent's solution that require existing SCPs to make changes and notifying each SCP of the required changes at least ninety (90) days prior to Commencement.
(xv) Train MSI and SCPs as applicable on the Successful Respondent's Services, systems, and SMM processes, focusing on the changes from the Incumbent Provider.
(xvi) Work with and create a schedule for all SCPs and the MSI to complete integration changes and ensure the accuracy of those changes.
(xvii) Test the accuracy of all integration points prior to Commencement.

## 2.5. Transition Project Plan

After Contract execution, the Successful Respondent will deliver an updated Transition Plan as a Critical Deliverable.

### 2.5.1. Transition Project Plan Proposal Requirements

The Successful Respondent shall use the proposed Transition Project Plan to create a consistent and coherent Transition management plan. The Transition Project Plan shall describe how the Successful Respondent will:

(i) Manage the Project.
(ii) Guide Project execution.
(iii) Document planning assumptions and decisions.
(iv) Work with the MSI to integrate into the MSI's systems.
(v) Facilitate communication among stakeholders.
(vi) Define key management review as to content, scope, and schedule.
(vii) Provide a baseline for progress measurement and Project control.

### 2.5.2. Transition Project Plan Critical Deliverable

(a) The Successful Respondent must submit and present to DIR a detailed Transition Project Plan for review, feedback, and approval on or before the date set forth in **Attachment 1.1 Deliverables**. The Transition Project Plan must include all phases of the transition for which the Successful Respondent has responsibility, including Deliverables and tasks as well as any tasks and dependencies that may be outside of the Successful Respondent's responsibility but may influence or relate to the Successful Respondent's work and ability to complete work as planned. In addition to maintaining steady-state operational capability, the Successful Respondent shall include any identified security concerns that will be addressed during Transition or any agreed upon Transformation Projects.

(b) After submission of the Critical Deliverable referenced in **Attachment 1.1 Deliverables**, the Successful Respondent must update the Detailed Transition Plan monthly, ensuring that the level of specificity of the plan for a forward rolling six (6) month period is defined to the task and named resource level. As an example, the initial project plan will include details for the first six (6) months and activity/milestone level (sufficient to track the overall progress of the program) for the anticipated remainder of the transition based on the current understanding of project scope and phasing.

(c) DIR will:

(i) Cooperate with the Successful Respondent to assist with and support the completion of the Transition as DIR finds necessary.
(ii) Assist the Successful Respondent in managing SCP facing efforts and cooperation with agreed Successful Respondent created roles, responsibilities, plans and requirements.
(iii) Approve or reject the completion of each phase of the Transition Plan in accordance with the acceptance criteria after written notice from the Successful Respondent that it considers such phase complete.

### 2.5.3. Kickoff

(a) The Successful Respondent, in conjunction with DIR staff, the MSI, and other impacted DCS SCPs, must plan and conduct a Project kickoff meeting presentation to the sponsors, key stakeholders, and

core project team after the mobilization effort. At a minimum, the presentation must include a high-level overview of the following:

(i) Project scope and schedule;
(ii) Goals of the Project;
(iii) Communications and regular meetings;
(iv) Methodology, approach, and tools to achieve the goals;
(v) Roles, responsibilities, and team expectations;
(vi) Tasks, Deliverables and significant work products; and
(vii) Risk, issue, resolution and milestone reporting.

(b) All Successful Respondent project team members will review and understand the Successful Respondent's role and their responsibilities under the Contract. Additionally, all Successful Respondent project team members and DIR and MSI project team members must participate in the kickoff meeting.

### 2.5.4. Meeting Attendance and Reporting Requirements

(a) The Successful Respondent's project management approach must align with the established Project Management processes documented in the Service Management Manual (SMM) and adhere to the following meeting and reporting requirements, unless otherwise agreed to by DIR:

(i) Immediate Reporting - The Project Manager or a designee must immediately report any Project staffing changes to DIR's Project Manager in accordance with Article 5 Successful Respondent Personnel Requirements.
(ii) Attend Weekly Status Meetings - The Successful Respondent's Project Manager and applicable Project team members must attend weekly status meetings with DIR's Project Manager and applicable members of the DIR Project team as necessary to discuss Project issues. These weekly meetings must follow an agreed upon agenda which is distributed by the Successful Respondent no later than forty-eight (48) hours before the meeting and allow the Successful Respondent and DIR to discuss any issues that concern them.
(iii) Provide Weekly Status Reports - The Successful Respondent must provide written status reports to DIR's Project Manager at least one (1) full Business Day before each weekly status meeting.
(iv) At a minimum, weekly status reports must contain the items identified below:

A. Updated Transition Project Plan files on electronic media acceptable to DIR;
B. Status of currently planned tasks - specifically, identifying tasks not on schedule and a resolution plan to return to the planned schedule;
C. Issues encountered, proposed resolutions and actual resolutions;
D. The results of any tests;
E. A Problem Tracking Report must be attached;
F. Anticipated tasks to be completed in the next week;
G. Task and Deliverable status, with percentage of completion and time ahead or behind schedule for tasks and milestones;

H. Proposed changes to the Project work breakdown structure and Project schedule, if any;
I. Identification of Successful Respondent staff assigned to specific activities;
J. Planned absence of Successful Respondent staff and the expected return date;
K. Modification of any known staffing changes; and
L. System integration/interface activities.

(v) Prepare and Lead Monthly Status Reports – During the Project, the Successful Respondent must submit a written monthly status report to DIR's Project Manager by the fifth (5th) Business Day following the end of each month. At a minimum, monthly status reports must contain the following:

A. A description of the overall completion status of the Project in terms of the approved Transition Project Plan (schedule and cost, if applicable);
B. Updated Project work breakdown structure and Project schedule;
C. The plans for activities scheduled for the next month;
D. The status of all Deliverables, with percentage of completion;
E. Time ahead or behind schedule for applicable tasks;
F. A risk analysis of actual and perceived problems, including recommended remediations and a red, yellow, or green status indicator;
G. Testing status and test results; and
H. Strategic changes to the Transition Project Plan, if any.

(b) The Successful Respondent's proposed format and level of detail for the status report is subject to DIR's approval.

### 2.5.5. Transition Documentation and Collaboration

The Successful Respondent must use the MSI Portal for document management and team collaboration. This hosted document management and team collaboration capability provides access through internal state networks and secure external connections to all project team members, approved project stakeholders, and participants. In conjunction with the utilization of this tool, the Successful Respondent must:

(i) Structure the document management and collaboration pages and data structures in such a manner as to deliver on the overall requirements of the Project; and

(ii) Load all Service-related documentation, deliverables, reference material and/or configuration documentation onto the MSI's document collaboration tool. The Successful Respondent must confirm with the MSI that all documentation has been provided and is readily available.

### 2.5.6. Determination of Responsibility (Successful Respondent and Other State Vendors)

The Successful Respondent shall be responsible for:

(i) Failures that are exclusively in the Successful Respondent's area of responsibility, or that are exclusively staffed or performed by Successful Respondent-provided personnel;

(ii) Failures where DCS Services personnel (MSI, SCP, or DIR) are following established Successful Respondent processes where, as a result of issues, defects, omissions, or inconsistencies in these designed and provided processes are shown to be the primary source of the failure;

(iii) Failures where DCS Services personnel (MSI, SCP, or DIR) are not provided processes that are the Successful Respondent's responsibility to design, develop, implement, or document;

(iv) Failures where Successful Respondent Services personnel has an exclusive role or responsibility and is not dependent on DIR resources to complete the tasks associated with the failure;

(v) Failures arising where DCS personnel (MSI, SCP, or DIR) are following the direction of a Successful Respondent resource where that direction is inconsistent with established policies and procedures;

(vi) Failures arising where a DCS resource is performing a role, responsibility, or task that is outside of the established DCS providers' responsibility but within the Successful Respondent's responsibility area on an ad hoc or temporary basis in lieu of a Successful Respondent resource at the request of the Successful Respondent;

(vii) Any failure arising from Successful Respondent personnel not following established State security, privacy or other IT policies;

(viii) Any failure resulting from a subcontractor working for, or at the direction of the Successful Respondent; and

(ix) Failures arising from Successful Respondent-owned equipment or computing devices coincident with providing the in-scope services.

### 2.5.7. Organizational Change Management

During Transition, the Successful Respondent will be required to document all functions and technologies of the organization. The Successful Respondent will be responsible for implementing and training all stakeholders on the following items, which should be documented in the SMM:

(i) Service Operational Processes and Procedures;

(ii) DIR Operations Service Team Change Management and Training; and

(iii) DCS Customer-, MSI-, or DCS SCP- facing equipment, tools, and processes required to satisfy the business, functional, and technical requirements.

### 2.5.8. Operational Readiness Assessment

The Successful Respondent will assess its readiness to assume operations and maintain the functionality deployed under this Exhibit. The Successful Respondent will recommend strategies as required to ensure DIR, DCS Customers, and DCS SCPs are prepared to support any new system functionality. The Successful Respondent will design the Service as to meet the criteria of the Operational Readiness Assessment Critical Deliverable, as defined in **Attachment 1.1 Deliverables**.

### 2.5.9. Staffing Plan and Time Commitment

(a) The Successful Respondent shall provide a summary of full time equivalent (FTE) personnel needed for transition of the Services along with Service design and implementation. Additionally, any

requirements of DIR, DCS Customers, MSI, or of the SCP(s) performing the current service, as well as delivery and space planning considerations, will be outlined in a Full Time Equivalent Personnel table.

(b) FTE time shall represent those hours in direct support of the Service. In some cases, this number may be less than 100%.

### 2.5.10. Remedies for Transition Failure

(a) In the event that Successful Respondent fails to identify and resolve any problems that may impede or delay the timely completion of each task in the Transition Plan, without prejudice to DIR's other rights and remedies under the Agreement or at law or equity,

(i) Successful Respondent will provide, at its sole cost and expense, all such additional resources as are necessary to identify and resolve any problems that may impede or delay the timely completion of each task in the Transition Plan, and

(ii) DIR may equitably reduce the Charges set forth in **Exhibit 2 Pricing** in an amount estimated by DIR to account for the Services that DIR and/or the DCS Customers are not receiving or did not receive.

(b) Successful Respondent represents and warrants to DIR that, as of the Commencement Date, it is ready to commence performing the Services in accordance with the terms of this Agreement, including with respect to pricing, applicable Service Levels and other performance obligations. In the event that such representation and warranty is not true and correct, Successful Respondent will reimburse DIR for any costs or expenses incurred by DIR as a result of the failure of such representation and warranty to be true and correct. In the event that Successful Respondent is required to perform any Transition activities following the Effective Date, Successful Respondent will complete such activities at its own cost and expense and in such a manner so as to not materially disrupt or cause any material adverse impact on DIR's operations or activities unless otherwise agreed to with DIR.

## 3. Security: Steady State Run Services

The following table cross references the requirements in Article 3 Security: Steady State Run Services to the seven (7) core Security Operations functional areas:

**Table 3: Security Operation Core Functional Areas**

| SOW Section | Description | Associated Core Functional Areas |
|---|---|---|
| 3.1. | General Requirements | Multiple |
| 3.1.1. | Security Incident and Event Monitoring (SIEM) | 4. Security Incident and Event Monitoring (SIEM) |
| 3.1.2. | Privileged Access Management (PAM) | 2. Privileged Access Management (PAM) |
| 3.1.3. | Firewall Rule Management | 1. Security Policies and Standards |

| SOW Section | Description | Associated Core Functional Areas |
|---|---|---|
| 3.1.4. | Cloud Access Security Broker (CASB): Standards and Alerts | 1. Security Policies and Standards |
| 3.1.5. | Advanced Malware Protection Standards | 1. Security Policies and Standards |
| 3.1.6. | Security Threat Identification and Remediation | 3. Vulnerability Management Program |
| 3.1.7. | Master Security Baseline Configurations Standards | 1. Security Policies and Standards |
| 3.1.8. | Establish Operating Procedures, Protocols and Coordination/Communication Mechanisms | 7. Program Management and Operations |
| 3.1.9. | Operation, Monitoring and Reporting | 7. Program Management and Operations |
| 3.2. | Security Program Management | 7. Program Management and Operations |
| 3.3. | Security Standards | 1. Security Policies and Standards |
| 3.4. | Security Auditing and Reporting Requirements | 7. Program Management and Operations |
| 3.5. | Ongoing DCS Security Operations Requirements | 7. Program Management and Operations |
| 3.5.1. | General Identification and Integration Requirements | 7. Program Management and Operations |
| 3.5.2. | State Enterprise Security System Operations and Integration | 7. Program Management and Operations |
| 3.6. | Managed Intrusion Detection, Management and Prevention Services | 4. Security Incident and Event Monitoring (SIEM) |
| 3.7. | Intentionally Left Blank | n/a |
| 3.8. | Security Emergency Response Services | 6. Incident Response Command |
| 3.9. | Security Vulnerability Identification and Remediation Services | 3. Vulnerability Management Program |
| 3.9.1. | General Scope of Security Vulnerability Identification and Remediation Services | 3. Vulnerability Management Program |
| 3.9.1.1 | Active Threat Identification | 5. Active Threat Identification |
| 3.9.2. | External Sources and Standards | 1. Security Policies and Standards |
| 3.9.3. | Vulnerability Identification Services | 3. Vulnerability Management Program |
| 3.9.4. | Vulnerability Identification Actions | 3. Vulnerability Management Program |
| 3.10. | Security Incident Management | 6. Incident Response Command |
| 3.11. | Risk Management and Tracking | 7. Program Management and Operations |
| 3.12. | Steady State Security Operations, Maintenance and Monitoring Requirements | 7. Program Management and Operations |

| SOW Section | Description | Associated Core Functional Areas |
|---|---|---|
| 3.12.1. | Routine Maintenance, Patching, Updates and Hot-Fixes | 7. Program Management and Operations |
| 3.12.2. | Level 2 and 3 Support Services | 7. Program Management and Operations |
| 3.12.3. | Emergency Break / Fix Support | 7. Program Management and Operations |
| 3.12.4. | Operations Reporting | 7. Program Management and Operations |
| 3.12.5. | Security Operations Support | 7. Program Management and Operations |
| 3.12.6. | Security Solution and Operations Reporting | 7. Program Management and Operations |
| 3.12.7. | Ad-Hoc Request Support Obligations | 7. Program Management and Operations |
| 3.12.8. | Security Systems Management and Administration | 7. Program Management and Operations |
| 3.13. | Cybersecurity Assessment | 3. Vulnerability Management Program |
| 3.14. | Disaster Recovery Support Services | 7. Program Management and Operations |
| 3.15. | Reporting | 7. Program Management and Operations |
| 3.16. | Compliance | 7. Program Management and Operations |
| 3.17. | Quality Assurance | 7. Program Management and Operations |
| 3.18. | Industry Standards, Certifications and Compliance | 7. Program Management and Operations |
| 3.19. | Obligation to Evolve | 7. Program Management and Operations |
| 3.20. | Operating Agreements with Other SCPs and MSI | 7. Program Management and Operations |
| 3.21. | Successful Respondent Cooperation | 7. Program Management and Operations |
| 3.22. | Onboarding New Customers | 7. Program Management and Operations |
| 3.23. | Performance Guarantee | 7. Program Management and Operations |

## 3.1. General Requirements

(a) **NOTE**: This scope of work does not include the scope for Managed Security Services (MSS) which is a service that DCS Customers may utilize in relation to their DCS and non-DCS environments.

(b) DIR has designed its operating model to leverage an MSI which currently operates on an ITIL-based platform with specific tools and processes that all SCPs are expected to use and align to. The MSI

provided tools are documented in the data room. Requirements related to these cross-functional processes and components are detailed in Article 9 Cross-Functional Services. To the extent Respondent's service delivery model does not align with ITIL framework, it is expected that Respondents will provide sufficient explanation for the reason for Respondent's departure from excepted ITIL practices and standards.

(c) The Successful Respondent's delivery of Security Management shall be an integral part of the other IT disciplines and deployed across all Service Components to ensure that security requirements are met and verified. Security Management shall assess all security risks and vulnerabilities associated with the delivery of Services are appropriately identified, evaluated, assessed and appropriate controls are implemented and maintained. Security shall also provide the tools, knowledge, and capabilities to provide security monitoring and identity management.

(d) DIR requires a production implementation and ongoing operation of security services including, but not limited to:

(i) Tools and tool integration with the Security Operations SIEM;
(ii) Privileged Access Management (PAM), and if approved, a transformation project to implement an IAM system that provides identity and access management across the DCS Enterprise;
(iii) Aggregation of monitored events and security incident handling including providing leadership to resolve Security Incidents;
(iv) Security risk and vulnerability management for aggregated events; and
(v) Establishment of operating methods and procedure.

(e) This effort must be designed, implemented and thereafter operated to be extensible to current and potential future DCS Customers as a DCS security service to:

(i) Enhance the detection of cyber threats affecting entities within the State of Texas DCS program;
(ii) Incorporate public cloud connectivity and threat protection for DCS Infrastructure, Platform and Software as a service (collectively IaaS, PaaS, SaaS) assets that connect with State DCS networks;
(iii) Incorporate DIR and augment cyber intelligence to the State in order to increase Cybersecurity defenses and information sharing with various government, education, and business organizations; and
(iv) Assist the State in response to State-level Cybersecurity events and incidents.

### 3.1.1. Security Incident and Event Monitoring (SIEM)

The Successful Respondent is responsible for defining and implementing SIEM tools and capabilities to track DCS service events and service notification workflows inclusive of:

(i) Implement a new SIEM tool (referred to as SIEM or Security Operations SIEM) for all DCS service components, assure data is being received into the SIEM from the other SCPs, and provide real-time integration of audit logs to the Security Operations SIEM solution for audit reporting, alerting and management by the Successful Respondent

and State Security and Privacy Personnel. The SIEM must be located within either the ADC/SDC or the continental United States if this is a cloud-based solution.

(ii) DCS service events exclude infrastructure components not hosted or managed by the DCS program, but any connections of unmanaged infrastructure components are monitored from the point they enter the DCS enterprise network.

(iii) Provide Security Operations SIEM integration design, implementation and operation inclusive of all tracked system events.

(iv) Integrate the SIEM tool with all DCS SCPs and MSI tools to ensure events are reported, monitored and correlated across discrete sources.

(v) Systematically evaluate scan output and findings to identify non-Standard or non-compliant operating systems, security software, user administration software and DCS software applications or versions to be the subject of migration to State Standards.

(vi) Perform validation, no less frequently than quarterly, that all required security events are collected, correlated and included in security alert and monitoring processes and applicable tools.

(vii) Elimination of all "false positive" events and events that are not security or threat related.

(viii) Provide ability for long term storage and retrieval of data based on DCS Customer regulatory requirements.

(ix) Provide automated SIEM reporting and notifications based on workflows and data sent to the SIEM by Respondent and other SCPs.

(x) Work with the MSI and DIR to confirm which events constitute a security incident and integrate the Security Operations SIEM electronically with the MSI ticketing system to log security incidents.

(xi) Provide electronic notification of high levels of Security Incidents or problems that meet State defined parameters and utilize existing notification protocols and capabilities such as text message, email and other common communications formats to communicate notifications.

(xii) Provide and execute a process for continual improvement, updating and tuning of the SIEM solution.

(xiii) Provide automated SIEM reporting as specified in Appendix A Reports, and data to the MSI using agreed upon interface methods to allow the MSI to provide overall reporting and dashboards, including but not limited to:

A. Produce audit reports via either Successful Respondent provided web reporting tools or access via MSI Portal (as dashboards and reports) and retain such information for no less than two (2) years.

B. Be capable of producing web accessible reports and dashboards with the ability to export the report in Excel CSV, XLSX, or PDF formats as appropriate to the content of the report and user needs.

(xiv) Retain SIEM logs for a minimum of two (2) years with three (3) months hot, nine (9) months warm and twelve (12) months cold data with a twenty-four (24) hour SLA response to move data from warm to hot and forty-eight (48) hours to move data from cold to hot as described in Section 7.3.15(b)(ii) System Auditing Requirements.

### 3.1.2. Privileged Access Management (PAM)

The Successful Respondent is responsible for implementing Privileged Access Management capabilities to manage all DCS privileged IDs. The Successful Respondent shall:

(i) Manage privileged access IDs used for all DCS SCPs, MSI, DIR, or DCS Customers that require privileged access to DCS services.
(ii) Provide, implement and operate the DCS Privileged Access Management (PAM) tool either using either DIR's Private Cloud or Gov Cloud instance.
(iii) Establish access management policies and procedures.
(iv) Track who used the accounts, including SCPs, MSI, DIR, DCS Customers, on which services or servers, reason for the access, and for how long.
(v) If the IAM project is approved, integrate the PAM system with the proposed IAM system for the automated creation, modification, suspension, and deletion of PAM accounts as needed.
(vi) Integrate the PAM system with the following:
    A. MSI ticketing system for automated PAM administration, and as needed manual administration;
    B. Directory services (DCS private cloud directory, DCS tools network directory, DCS mainframe directory, AWS public cloud directory, Azure public cloud directory, DCS Customer directory);
    C. Security Operations Multi Factor Authentication;
    D. Security Operations vulnerability management solution;
    E. Security Operations SIEM.
(vii) Provide automated controls that allow for the secure check-in and check-out of any shared accounts.
(viii) Provide optional recording of sessions using PAM depending on DCS Customer needs for adherence to regulatory requirements.
(ix) Integrate with the SIEM to record the usage of a PAM account and allow correlation of the user, the account, events, and actions taken.
(x) Integrate SCP Multi Factor Authentication (MFA) solutions with proposed PAM solution.
(xi) As directed by DIR, participate in security audits of the DCS program, providing documentation of security access controls.
(xii) Provide MSI and DIR with security access policies and procedures compliance reporting.

### 3.1.3. Firewall Rule Management

The Successful Respondent shall:

(i) Lead the coordination of firewall rules within the DCS environments and between the MSI and SCPs.
(ii) In coordination with the MSI and related SCPs, design and lead the integration of firewall policy management and automated firewall rules management within the MSI operated Service Catalog, request workflow and SCP API's.

(iii) For Firewall Rule administration that is not yet automated, lead the SMM process development efforts and coordinate with the MSI and related SCPs to design and document the administration of firewall rules management security.

(iv) Manage firewall rule deployment to all environments where the operating SCP has provided automation and an abstracted level of access to the environment that appropriately separates administrative and operational functions from firewall rule management. Where this condition has not been met, the operating SCP is responsible for performing firewall rule management.

### 3.1.4. Cloud Access Security Broker (CASB): Standards and Alerts

The DCS CASB will be designed to ensure that network traffic between on-premises devices and any public cloud provider complies with the DCS and State of Texas (TAC 202) security policies and will provide real-time access via reports, dashboards and alerts. The Successful Respondent will establish, publish and maintain CASB standards for use in the DCS public cloud environments. The Public Cloud Manager SCP will be responsible for purchasing and deploying the CASB in accordance with the Successful Respondent's required standards.

#### 3.1.4.1. CASB Standards

The Successful Respondent shall:

(i) Design, establish, and publish to the SMM, written standards for a DCS enterprise Cloud Access Security Broker (CASB) for use with data and systems that are maintained in any public cloud infrastructure (IaaS), platform (PaaS) or software (SaaS) environment.

(ii) The standards shall include but are not limited to the following topics:

A. Auto-discovery of cloud applications and data in use in order to identify high-risk applications, high-risk users and other key risk factors as determined by DIR or DCS Customers who maintain or have access to restricted or protected data.

B. Enforcement of the most stringent of applicable Texas Security, DCS Security Policy or DCS Customer specified security access controls, including: encryption; device and access profiling; and credential mapping when DCS Identity and Access Management (single sign-on) is not available or utilized on the public cloud provider platform.

C. Identification of all cloud services in use (approved, unapproved or "shadow"), by whom, and what risks they pose to the DCS program as well as DCS Customer data and systems maintained in public cloud providers.

D. Inventory or database of cloud services and their security controls including which controls are implemented or absent as to help DCS Customers increase the security controls pertinent to their public cloud environment(s).

E. Protection of DCS program and Customer data in the cloud by preventing certain types of sensitive data from being uploaded, and encrypting and tokenizing data.

F. Identification of potential misuse of cloud services, including both activity from insiders as well as third parties that compromise or circumvent establish DCS standards pertinent to user accounts.

G. Enforcement of data access and cloud service functionality based on the user's device, location, and operating system as well as "role" within the organization (e.g., privileged access, trusted access, operational access, end-user or general public access).

(iii) Communicate requirements and standards to the DCS Public Cloud Manager SCP for implementation by the DCS Public Cloud Manager SCP for all DCS program public cloud provider elements.

#### 3.1.4.2. CASB Alert Integration and Oversight

The Successful Respondent shall:

(i) Integrate CASB-generated alerts with the Security Operations SIEM to identify all uses, and alert on suspicious or inappropriate cloud application use across cloud platforms and identity unsanctioned use inclusive of restricted or protected data, network, or application/service access of State data and systems maintained within public cloud providers.

(ii) Review the RFS and solution designs and implementation specifics based on the DCS Public Cloud Manager SCP selected system(s) to achieve CASB requirements.

(iii) Include in these requirements all necessary integrations for alerts, alarms, reports and dashboards as to ensure that DIR and DCS Customers are provided the required information to ensure the correct configuration, implementation and operation of CASB elements for public cloud elements of the DCS program.

(iv) Participate in acceptance testing and review of DCS CASB element(s) prior to DIR acceptance of same, and document any deviations, defects or omissions from the scope of the DCS CASB as implemented.

### 3.1.5. Advanced Malware Protection Standards

The Successful Respondent shall provide Malware protection standards including:

(i) Provide leadership across all SCPs to improve the security posture of DCS Services including ensuring a comprehensive solution to protecting DCS computing and storage Services from Malware is operated within the DCS service.

(ii) Ensure that solutions used within DCS and are optimized for the protection of Malware risks for each discrete environment within DCS.

(iii) Create and communicate enterprise standards for all DCS computing assets as to best protect DCS Customers from any gaps/omissions in the endpoint community and as to "layer" additional protections for DCS assets.

(iv) Provide unified policies, standards, and integration into SIEM processing and reporting.

(v) Provide DIR with the required visibility into the number or severity of infections that occur such that the SCPs, Customers, MSI, and DIR can take defensive measures to

prevent malware infections from spreading from one agency to another (in general) and from one DCS asset to another (specifically).

### 3.1.6. Security Threat Identification and Remediation

The Successful Respondent shall:

(i) Provide proactive identification of cybersecurity risks, including privacy risks, and attacks including ones the State of Texas has previously not been able to detect inclusive of SCP and MSI provided feeds, and NSOC and OCISO subscribed threat intelligence feeds.

(ii) Work with the MSI to integrate security threat identification and remediation processes into the MSI-lead cross-functional processes.

(iii) Validate DCS SCP intrusion detection and intrusion prevention capabilities are performing to approved standards and provide recommendations to mitigate deficiencies.

(iv) Identify high-risk system elements and include identification of them in SCP intrusion detection system elements, hardening, isolation and other prevention method standards.

(v) Perform programmatic analysis and detection of incidents or persistent access attempts that include confirmation and assessment of risks.

(vi) Perform rapid methods to identify, contain and remediate active threats.

(vii) Support the enhancement to security and operational policies and procedures and operating model changes to eliminate security exposures in the DCS environment.

(viii) Develop and execute methods to assist the State and DCS participants in predicting future threats and access attempts and proactively address concerns before they become active.

(ix) Provide on-going threat reports and alerts for DIR, the MSI, and SCPs so that risks are identified and appropriately mitigated.

### 3.1.7. Master Security Baseline Configurations Standards

(a) The Master Security Baseline Configurations (MSBC) reflects the security responsibilities and practices required for the DCS program with the goals of hardening, standardizing, and integrating DCS Security across all the DCS Service Components. The document lists the technical control settings and standards as agreed to by DIR. The Successful Respondent is required to define and maintain the MSBC for the DCS SCPs. The Successful Respondent shall update the MSBC initially after Commencement, and annually per **Attachment 1.1 Deliverables** and include as part of the Successful Respondent's contribution to the Annual Security Plan per **Attachment 1.1 Deliverables**. The Successful Respondent will then notify the Texas Private Cloud and Public Cloud Manager SCPs and oversee their implementation of the new baselines.

(b) The Successful Respondent will also ensure the SCPs, on a quarterly basis, run healthcheck scans against the baseline configurations and report to each customer where their compute does not meet the minimum standards. The Successful Respondent is responsible for evaluating these gaps, advising customers on appropriate mitigations, and processing customer exception requests for DIR final approval.

(c) The Successful Respondent will design, implement extensible Security standards documented in the MSBC upon DIR approval that include:

(i) Hardening of DCS Services inclusive of devices, hardware, software, configuration and integrations, validation, technical, testing and other details pertinent to the State or a capable third party of the State's choosing to incorporate the features, functions and capabilities developed for the DCS Service.

(ii) Any and all DCS integrations, configurations, extensions, workflows, conversions and other elements pertinent to the operation, maintenance or extension of intrusion and fraud detection elements associated with the Services including operation manuals, release notes, test cases and results, technical contacts and documentation as provided or utilized in performing the Service.

(iii) The security standards, policies, and controls that the DCS SCPs will provide to DIR and DCS Customers.

(iv) Establishment of enterprise level requirements for passwords across the DIR Shared Services environment in cooperation with the Service SCPs and as part of the Security Program.

(v) Roles and responsibilities, services, and technical control settings and standards as agreed to by the Successful Respondent, DIR and DCS Customers.

(vi) Security settings along with associated baseline data, agreed to settings, gap analysis, and threat identification activities to communicate known vulnerabilities in the DCS Customer security environment.

#### 3.1.7.1. MSBC Management

The Successful Respondent shall manage the MSBC standards and processing, including:

(i) Provide updates to the MSBC document as required by the Successful Respondent and/or DIR and DCS Customers, with a re-issue at least every twelve (12) months. DIR will approve all updates, changes, modifications, and re-issues.

(ii) Coordinate and aggregate quarterly MSBC Health Checks.

(iii) Collect and utilize SCP-run scans quarterly that will feed baseline information to the Successful Respondent to determine the health check of the system.

(iv) Aggregate SCP health check information into the DIR GRC tool (currently SPECTRIM) through an agreed interface (e.g., .csv SFTP and/or GRC tool direct query of MSI system).

(v) Integrate management of the configurations into the DIR GRC tool to provide DCS Customers with the ability to manage exceptions with automated workflows. Identify expiring exceptions and notify DCS Customer in advance of the expiration.

### 3.1.8. Establish Operating Procedures, Protocols and Coordination/Communication Mechanisms

The Successful Respondent shall develop or update the SMM to address and include the following:

(i) Ensure communication and resolution of identified security threats.

(ii) Ensure continued close integration and information sharing with State and Federal Threat Intelligence Agencies as currently performed by the DIR NSOC and OCISO functions.

(iii) Compliance and monitoring model for the services.
(iv) Efficient method for onboarding future participating entities.

### 3.1.9. Operation, Monitoring and Reporting

Successful Respondent shall:

(i) Provide 24x7x365 cyber threat intelligence and monitoring services.
(ii) Provide weekly threat and incident reports to the State, and daily reports of active or persistent threat attempts.
(iii) Confirm there is no degradation of Internet traffic to and from the State of Texas as a result of the services.
(iv) Understand and determine the merits of integrations and enhancements to requirements for of the "Texas cybersecurity threat map" utilized at the NSOC that can be updated near real-time by the service provider to indicate threats affecting or originating from Texas entities.
(v) If elected by DIR, upon implementation, operate the Identity and Access Management System Service for the DCS Program.
(vi) Confirm the ability to selectively parse traffic to optional services as to provide extended security services to specific network traffic types.

## 3.2. Security Program Management

(a) The Successful Respondent shall develop and operate an overall Cybersecurity risk management program including vulnerability management based off NIST standards that integrates with the Shared Services' Risk Program(s).

(b) The Successful Respondent shall, at a minimum:

(i) Lead the SCPs in the development, implementation, and maintenance of a Security Program, which will comprise on-going activities of DIR, DCS Customers, and SCPs.
(ii) Establish an on-going Security Program that meets the external requirements according to security policies, contractual requirements, legislative requirements, TAC 202, and the requirements defined in this document.
(iii) Develop, maintain, update, and implement security procedures and Service Responsibility Matrices with DIR, the MSI, and DCS Customer's review and approval, including physical and logical access strategies and standards.
(iv) Assist DIR and DCS Customers in implementing security requirements and coordinating with the MSI and SCPs.
(v) Bring subject matter expertise in security requirements, such as PCI or IRS 1075, to assist customers to achieve compliance with security laws, rules and regulations.
(vi) Perform security evaluations as directed by DIR, which include conducting internal audits, supporting external audits, conducting self-assessments, and evaluating security Incidents.
(vii) Lead the resolution of security issues across the SCPs to ensure issues are resolved.
(viii) Coordinate Security Management activities across all SCPs that provide services to DCS Customers.

(ix) Conduct regularly scheduled Security Management meetings.

A. Document and publish meetings status reports to all relevant stakeholders, including DIR, DCS Customers, MSI, SCPs, and authorized Third Party Vendors.

B. Coordinate resolution of agreed-to activities resulting from Security Management meetings.

C. Evaluate the effectiveness of Security operations management across all SCPs. Recommend improvements to DIR and SCPs.

(xiii) Working with DIR and the MSI, maintain the overall Security Incident Management Plan, defining roles and responsibilities across DIR, MSI, Customers, and Service Component Providers.

A. Obtain and consolidate the plans and exceptions documented for all Security Incident Management Plans, including security Incident priority matrix, notification rosters, communications plans, and procedures for managing security Incidents.

B. Implement the Security Incident Management Plan in concert with participation from the required MSI, Service Component Provider and Customer personnel.

C. Coordinate Security Incident Management procedures with the MSI's Major Incident Management procedures.

(xiv) Provide for 24x7x365 security monitoring and reporting on Security events across the enterprise.

(xv) Ensure all systems and applications that the Successful Respondent uses to support DIR and DCS Customers are in a supported and secure state.

(xvi) Establish and manage a NIST-based vulnerability management program across all SCPs and Successful Respondent-provided systems.

(xvii) Where SCPs are required to run vulnerability scans, work with the MSI to ensure the scans are run monthly and ensure that vulnerabilities are received and analyzed by the Respondent, and vulnerabilities are reported to the associated MSI, SCP, DCS Customer(s) for action.

(xviii) Track status of identified vulnerabilities and risk mitigation actions, reporting, and managing stakeholders to respond and eliminate identified vulnerabilities, where vulnerability levels to be tracked are specified and defined in the SMMs.

(xix) Provide DIR, through the MSI reporting process, with a monthly status of DIR Shared Services risk and vulnerability management.

(xx) On a quarterly basis, perform a review of all users assigned access to Successful Respondent systems and confirm access validity providing report to DIR.

(xxi) Provide a forward-looking schedule for the planned Security testing, assessments and analysis.

(xxii) Provide a detailed description of the potential benefits and exploitation opportunities that exist for planned technology upgrades and new solution opportunities based on technology evolution or changes in the threat landscape, including a description of anticipated Security benefits and the effort required to realize these benefits.

(xxiii) Develop and maintain a DIR-approved Security Program Operations Manual defining the workings of the security program and explaining how the Successful Respondent

shall manage risk across the SCPs following the NIST-based approach of continuous monitoring (at a minimum NIST SP 800-137) and incorporates, at a minimum:

A. The scope of Security Management, in terms of the services supported, the systems, environments, Operations Documents, Equipment, Software, and Applications, etc.
B. The policies, processes, procedures, roles and responsibilities, and activities that ensure the success of Security Management.
C. The systems and tools that support Security Management.
D. Integration and relationships with SCP and Successful Respondent Security Management.
E. How the success of Security Management will be monitored, measured and reported.
F. How 24x7 security monitoring and reporting on Security events will be supported.
G. Measure actual Security provided versus agreed-to levels of Security.
H. How continuous monitoring is achieved. How NIST-based Cybersecurity Risk Management is achieved and integrates into the overall DIR Program-level Risk Management.

## 3.3. Security Standards

(a) The Successful Respondent is to establish security standards for DCS inclusive of servers, network equipment and any other end point on the DCS network. Security standards must comply, at a minimum, with the following technical standards and requirements:

(i) Work with DIR to establish DCS security standards for use of TSS, MSI and SCPs throughout the program.
(ii) Ensure security standards protect against leaks of State restricted information such as personally identifiable information (PII) or design diagrams containing sensitive/intellectual property (IP), as to reduce the chances of a data breaches and maximize compliance with Federal and State regulations as Payment Card Industry (PCI), Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA), IRS1075 and other restricted data types.
(iii) Provide for a secure channel supporting real time data transmission between DCS Customers and the DCS Security Service, DCS SCP(s); DCS supported networks and demarcation/handoff points.
(iv) Comply with hardware and software manufacturer standards and best practices as to maximize operational efficiency and support.
(v) Provide for standards-based web services technology, including but not limited to SOAP, WS-Security, and XML, wherever possible to maximize integration and minimize “one-off” integrations and manual workarounds.
(vi) Be in compliance with all Federal standards and guidelines, and future evolutions thereof, including:
    A. Then current State Security, Privacy and Data Handling/Protection Policies (TAC 202 and Texas Cyber Security Framework)

B. CJIS Security Policy Resource Center standards, requirements and policies (https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center)
C. OMB M 04-04: E-Authentication Guidance for Federal Agencies;
D. NIST SP 800-63: Identity Proofing at Assurance Level 3;
E. FIPS 140-2: Encryption for backend data verification calls;
F. NIST SP 800-30: Risk Management Guide for Information Technology Systems;
G. NIST SP 800-95: Secure Web Services for backend data verification calls; and
H. Audit and Logging Requirements.

(b) The Service must provide full and configurable auditing capabilities, including the creation/deletion of Administrative Users (i.e., those users with administrator, root, pseudo or other privileged access to DCS service elements), password resets, role/privilege assignment, token assignments, multi-factor method(s) and devices, etc.

(c) For services provided to any DCS Customer, ensure that all personnel that provide such services meet all required CJIS requirements inclusive of background checks.

(d) System must provide full auditing of Administrative Users access to Service applications, resources, and individual user accounts.

(e) All auditing logs must be reviewable by state security administrators and security policy staff using access to system logs and via the programmatic fraud detection system(s) proposed by the Successful Respondent.

(f) The Service must support real-time replication or integration of no less than two (2) years of audit logs to the Security Information and Event Management (SIEM) solution (currently McAfee) security platform for audit reporting, alerting and management by State Security and Privacy Personnel that are retained and available for a period of no less than two (2) years and provided to DIR upon request.

(g) The Service must be configurable for auditing events and be extensible to support situational analysis of events and breeches (active and retrospectively) as to support incorporation of new rules, methods, tools and techniques to further enhance the State's overall security posture in the future.

(h) All Service activity must be attributed and logged to a single, unique system user.

(i) The Solution must support and be implemented with a failover configuration to ensure high availability.

(j) The Solution must not have a single point of failure.

(k) The Solution must support full back up and restore capabilities so the Solution (inclusive of software elements, data, configuration value and other elements as required to operate the Solution) can be restored from media with minimal additional intervention.

(l) The batch and backup operations must not degrade the response times of the system in off hours, assuming a lower request load to be estimated and justified by the Service Provider.

(m) The Successful Respondent hosted Primary Production and Disaster Recovery sites and all State data must be in the United States and located as to be technically diverse from the primary production site. Technical diversity factors include at a minimum: alternative and redundant power providers or grids, telecommunications network providers to those servicing the primary and disaster recovery sites respectively. This requirement can be met by hosting primary production and disaster recovery within the DCS program, although hosting at the DCS consolidated data centers is not required.

(n) The Successful Respondent must execute annual DR testing for elements they provide as part of the Service and provide the State with documented results and a remediation plan with committed resolution dates for any item identified as a weakness, material or otherwise from a technical, process, procedural or organizational perspective as provided to the State by the Successful Respondent under this Exhibit.

## 3.4. Security Auditing and Reporting Requirements

(a) The Successful Respondent will produce a monthly audit and compliance report for all DCS Service Assets that includes any identified vulnerabilities identified via continuous monitoring and Successful Respondent concerns with regard to:

(i) Inventory of Authorized and Unauthorized Devices upon discovery by the Successful Respondent;

(ii) Inventory of Authorized and Unauthorized Software upon discovery by the Successful Respondent;
(iii) Secure Configurations for Hardware and Software on DCS service provider, and Server, and service elements;
(iv) Secure Configurations for DCS Devices such as Firewalls, Web Application Firewalls (WAFs), Routers, and Switches, computing platforms, storage, mainframes and infrastructure;
(v) Boundary Defenses;
(vi) Maintenance, Monitoring, and Analysis of Security Audit Logs;
(vii) Application Software Security;
(viii) Controlled Use of Administrative Privileges via Privileged Access Management;
(ix) Controlled Access Based on Need to Know;
(x) Continuous Vulnerability Assessments and Remediation;
(xi) Account Monitoring and Control;
(xii) Taking action on Malware alerts from SCP tools;
(xiii) Limitation and Control of Network Ports, Protocols, and Services (Firewall Rules);
(xiv) Collaborate with any provider performing Texas required Penetration Tests and Red Team Exercises performed via the MSS vendor or by the State;
(xv) Incident Response Capability Assessment and recommendations for improvement to DIR and the MSI;
(xvi) Security Skills Assessment and Suggested Training to Fill Gaps.

(b) This report must contain DCS Customer name and device specifics as to effectively identify the DCS service element that is not in compliance or of concern, the DCS customer and the appropriate DCS SCP(s) required to address the issue.

## 3.5. Ongoing DCS Security Operations Requirements

(a) The Successful Respondent, as part of ongoing DCS security operations will:

(i) Detect, respond to (including notification of MSI and system custodians), and notify the appropriate SCP to remediate Security Incidents by analyzing intelligence and system logs, evaluating security telemetry, and leveraging intelligence feeds including:
(ii) Create incident tickets after the Solution or State detects an incident or an in-scope manual submission of an incident in the MSI service portal and SPECTRIM.
(iii) Identify incidents rated high Security severity (as mutually defined with the State, generally those that present an active or persistent threat) must be communicated to the State within 15 minutes after the incident is confirmed, as defined in the SMM.
(iv) Identify medium severity (as mutually defined with the State, generally those that present a high risk, but not active threat) incidents must be communicated within 1 hour after the incident is confirmed, as defined in the SMM.
(v) Coordinate and manage the incident, which includes communicating with DIR NSOC's Incident Response Team throughout the incident management lifecycle (detection, investigation, mitigation, remediation).
(vi) Provide notification to the State the incident has been resolved or remediated and document the same via the MSI service portal and SPECTRIM.

(b) In collaboration with the State, determine a categorization for incidents using the TAC 202, US-CERT and other DIR guidelines including:

(i) Working with the MSI, a defined communication and coordination processes including procedures and templates as required, such as; State internal use; between the State and Local/Municipal Governments; within the Local Government community; between the State and the Education Community; within the Education community; and within the Private Sector if reported to the State.
(ii) SLAs and incident risk ratings based upon these categorizations must be defined and agreed for the Service.
(iii) Develop and over the life of the Service evolve standards (for State review and approval) to define severity, and close-out of all incidents.

### 3.5.1. General Identification and Integration Requirements

Should the Service determine that one (1) or more of: 1) a known fraudulent access attempt; 2) apparent fraudulent activity; or 3) suspicious activity or traffic the Successful Respondent's provided Solution shall:

(i) Open a Priority 1 Security Incident and follow established communication protocols, as defined in the SMM;
(ii) Suspend access to the impacted service element(s), if actual behavior is outside of expected range or if the user appears suspect;
(iii) Remand attempted access to the system to the State to conduct further review and investigation of the traffic, transaction or user, as warranted; and
(iv) Initiate applicable MSI, DCS or DCS Customer specific workflows related to suspending, limiting, blocking or if necessary terminating access inclusive of (at the State request) remanding the access or attempted access to data to State or Federal authorities as determined.

### 3.5.2. State Enterprise Security System Operations and Integration

(a) As new systems or DCS elements are brought online, the Successful Respondent will conduct requirements and design sessions with the State security group to establish a definitive set of "security events" that are to be added to the Successful Respondent proposed network analysis, logging and intrusion detection solution.

(b) The Successful Respondent will work with the required SCPs to implement integration between DCS elements and services and the Successful Respondent's Security Operations SIEM, and, ensure the DCS elements are integrated into the MSI event management system.

(c) Support the State in the development of security alerts, warnings, programmatic system actions (e.g., suspend system, network or user access, require re-validation of IDs, alert DCS Customer and DIR security staff) and other features as required to support the State in identifying intrusive or inappropriate access to State systems. This will result in the State being able to take action as required within the context of State systems, networks, computing platforms, and other means as to minimize the State's exposure to intrusive, unapproved, or inappropriate access.

(d) The solution must support real-time replication or integration of auditable events to the respondent's Security Operations SIEM solution.

## 3.6. Managed Intrusion Detection, Management and Prevention Services

### 3.6.1. Service Scope Requirements

(a) Successful Respondent shall support service demarcation/handoff points for implementation and management of the following services as part of the service. The technical scope of the Service shall include the following:

(i) Security Event Identification and Alerting Services;
(ii) Aggregation and monitoring of SCP intrusion services;
(iii) Web Security Services; and
(iv) Security Data Analytics.

(b) The Successful Respondent will establish a definitive set of functional and technical requirements for the technical scope of service, enabling the service to function across the SCPs. The SCPs will deploy and provide the SCP-level IDS/IPS service that should feed alerts to the Successful Respondent's SIEM.

(c) To receive alerts to the SIEM, the Successful Respondent will design, implement and maintain all elements required for operation in a production environment inclusive of any of the following:

(i) Security Software and Monitoring Tool Software;
(ii) Security Analytics and Correlation Software and Tools;
(iii) Operational Processes and Procedures;
(iv) State Security operations team Change Management and Training;
(v) DCS Customer Change Management and Training;
(vi) SCP Monitoring and Alerting Tools integration with the Security Operations SIEM; and

(vii) Other equipment, Tools, Processes required to satisfy the State's business, functional and technical requirements contained in this Exhibit.

### 3.6.2. Operational Support Requirements

(a) The Successful Respondent will be responsible for:

(i) Command, control, 2nd/3rd level services, oversight; including process and procedures for State approval;
(ii) 24x7x365 intelligent monitoring of network intrusion detection and prevention devices;
(iii) Ongoing tuning and implementation of new filter sets after validation testing with the State as to not diminish the flows of legitimate network traffic;
(iv) Expert knowledge of the management and configuration of network intrusion detection and prevention devices;
(v) 24x7x365 access to Respondent's security experts via the MSI service portal;
(vi) Escalation of Security Incidents via email, phone and the MSI service portal and SPECTRIM;
(vii) Escalation of security event data via the MSI service portal;
(viii) Incident reports providing the DCS Customers and providers with actionable information following each escalation;
(ix) Reporting via the MSI service portal including high-level reporting (e.g., dashboards) and in-depth reporting on the security of DCS networks and attached devices;
(x) Vulnerability management including all network sensors, aggregation, correlation and console devices;
(xi) Security policy configuration changes applicable to attacks; and
(xii) DCS Customer and DIR requested policy configuration changes based on evolutions of State security policies.

(b) The proposed Service must be designed, implemented and deployed to:

(i) Support electronic notification of high levels of programmatic fraud attempts that include malicious or suspicious traffic that meet State defined parameters and utilize existing notification protocols and capabilities in the State such as text message, email and other common communications formats; and
(ii) Be capable of integrating into operational consoles utilized to protect State physical, logical, virtual, infrastructure and interconnection with public-cloud provider level DCS Customers and State responsible parties. By way of an illustrative use case: alert a State system or security manager via email that his/her system is under attack or probing via fraudulent access, credentials or other means.

## 3.7. Intentionally Left Blank

## 3.8. Security Emergency Response Services

(a) The Successful Respondent will be responsible for:

(i) Command, Control, 2nd/3rd Level services, Oversight; create process and procedures for State approval;

(ii) Provide emergency response twenty-four (24) hours/day, seven (7) days/week;

(iii) Upon receiving DCS Customer or Service Component Provider call or email for an emergency incident declaration using existing DCS incident response procedures (e.g., active intrusion or persistent threat), lead communications with DCS designated personnel, DIR and the MSI to discuss the symptoms DCS participant is observing, actions taken and similar items;

(iv) Provide assistance and advice for handling the emergency incident declaration including:

A. analysis of Security Incident data to determine the source of the incident, its cause, and its effects;

B. advising the relevant SCP and customer how to prevent the effects of the Security Incident from spreading to other DCS systems and networks;

C. advising the relevant SCP how to stop the Security Incident at its source and/or protecting DCS systems and networks from the effects of the Security Incident;

D. recommendations for restoration of the affected systems and networks to normal operation; and

E. suggesting protection methods for DCS systems and networks from future occurrences of the Security Incident;

(b) Prepare and provide an after-incident Report to the State describing the Security Incident, causes and effects, actions taken by the Successful Respondent, and recommended future actions to mitigate risk.

(c) Upon mutual determination of need, integrate data feeds, incidents, and alerts as part of a systems integration effort with the MSI's ServiceNow solution to ultimately enable updating the Respondent's data in SPECTRIM.

## 3.9. Security Vulnerability Identification and Remediation Services

Security vulnerability identification and remediation services include requirements pertaining to either or both of: rapid response to active, suspected or recurring attempts at accessing DCS infrastructure; and support of the remediation of Security deficiencies discovered or identified by the work as a result of State penetration testing or via other means as determined by the State in the course of operating and maintaining the infrastructure associated with DCS.

### 3.9.1. General Scope of Security Vulnerability Identification and Remediation Services

The Successful Respondent will, as part of the Service, be responsible for designing, implementing and providing the following Services:

#### 3.9.1.1. Active Threat Identification

**Active Threat Identification** should be designed and executed as to facilitate rapid remediation of active threats that are attempting to, or in fact have, compromised critical DCS infrastructure or computing assets as well as identify the potential scope and exposure of any State information to unauthorized parties. Due to the nature of these threats, the Successful Respondent's sole focus shall be to eliminate the State's DCS security exposure as expeditiously as possible by working through the SCPs and MSI, and

then lead subsequent root cause, reporting and related secondary remediation activities as secondary priorities.

#### 3.9.1.2. Vulnerability Identification

**Vulnerability Identification** should be designed and implemented to verify and remediate vulnerabilities regardless of origin (e.g., customers, customer environment, external parties, MSI, DCS SCPs, etc.) that, if exploited, may result in an intentional or unintentional compromise of a DCS system or infrastructure element and potential risks posed by known vulnerabilities, ranked in accordance with the National Vulnerability Database (NVD)/ Common Vulnerability Scoring System (CVSS) base scores associated with each vulnerability.

#### 3.9.1.3. Penetration Vulnerability Identification

(a) **Penetration Identification** should be designed to identify and potential penetration vulnerability methods, verify each method, and provide a standardized response. The Successful Respondent will provide a description of each vulnerability identified and/or potential issue remediated. Examples include but are not limited to SQL injection, privilege escalation, cross-site scripting, or deprecated protocols.

(b) The Successful Respondent shall propose tools, methods, and experienced personnel and lead the coordination of the response of other DCS SCPs (as part of a comprehensive response capability for DCS that includes:

(i) Application and Infrastructure Level Remediation;
(ii) Authentication, Roles and Permissions Remediation;
(iii) Web Applications and Mobile Access Remediation;
(iv) Remediation between segments of DCS Infrastructure Elements, Systems and Application Tiers; and
(v) Elements to remediate issues originating through Third-Party Hosted and Public or Private Cloud Environments.

### 3.9.2. External Sources and Standards

(a) Wherever possible, the Successful Respondent (in addition to Successful Respondent specific or proprietary elements) will incorporate the use of the NVD which is the U.S. government repository of standards-based vulnerability management data. This data is designed to enable automation of vulnerability management, security measurement, and compliance (e.g., Federal Information Security Management Act (FISMA)). In addition, the following industry standard references should be included as applicable:

(i) Common Vulnerabilities and Exposure (CVE);
(ii) Common Weakness Enumeration (CWE);
(iii) Bugtraq ID (BID); and
(iv) Open Source Vulnerability Database (OSVDB).

(b) Wherever possible, the Successful Respondent (in addition to Successful Respondent specific or proprietary elements) will incorporate the use of the CVSS which is designed to provide an open

framework for communicating the characteristics and impacts of IT vulnerabilities and remediation activities.

### 3.9.3. Vulnerability Identification Services

The Successful Respondent shall:

(i) Identify methods for manual method attack(s) and test(s);
(ii) Identify applicable remediation methods for automated or script-based attack(s) and test(s); and
(iii) Identify applicable remediation methods for attempts at gaining access via social engineering using a variety of public and/or State provided details to augment manual and/or automated methods.

### 3.9.4. Vulnerability Identification Actions

(a) The Successful Respondent will, within the scope of DCS and on a monthly basis, via internally (white box) and externally (black box) scanning:

(i) Identify applicable manual method attack(s) and test(s);
(ii) Identify and communicate all applicable manual, automated or script-based attack(s) exploit vectors or methods;
(iii) Verify the methods used to remediate the State infrastructure or systems element are in-fact performing as to defeat the attack, exploit vector or method;
(iv) Notify the affected DCS Customers and SCPs via MSI and DIR approved method(s) of all detected vulnerabilities; and
(v) Complete all agreed to steps and methods under the DIR-agreed General Method of the remediation for the Respondent's systems, some of which may require customer or DIR approval prior to implementing.

(b) **Under no circumstances shall the Successful Respondent remove any State data in performing work without the written consent of the DCS Information Security leader.**

(c) Provide the Confidential Vulnerability and Remediation Report quarterly, which shall contain:

(i) All Success/Failures and Issues or Weaknesses verified and remediated during performing the Service;
(ii) Verification that method(s) of Obtaining Access and (to the extent possible) a Root Cause Analysis have been addressed;
(iii) Position statement containing relative exposure details (e.g., system access, data access, privileges, elements exposed, duration and other pertinent details);
(iv) Verification of integration with the MSI vulnerability management console; and
(v) Ensure that if State data is acquired during remediation verification testing, it must be kept to a minimum and not listed in any report.

## 3.10. Security Incident Management

The Successful Respondent shall, at a minimum:

(i) Work with the MSI to develop Security Incident handling and notification processes that follow current NIST guidelines.
(ii) Leverage the MSI Major Incident Management (MIM) process and MSI MIM resources in order to coordinate and control accurate communication and efficient research involving multiple SCPS as well as DCS Customers and Third Parties.
(iii) Communicate and train DIR, DCS Customers, MSI, and SCPs on the Security Incident Management process ensuring consistent, effective detection, recording, investigation, diagnosis, and resolution of security Incidents.
(iv) Lead security incident response lifecycle from identification through resolution and root cause analysis.
(v) Direct the investigation, resolution, and closing of Security Incidents across the SCPs within the MSI's incident management framework.
(vi) Work with the MSI, DIR, SCPs, and Customers to escalate incidents that are not being resolved expeditiously or accurately.
(vii) Lead the incident response and investigation including performing forensic evidence gathering and initial analysis to understand incident scope and impact.
(viii) Manage information security containment.
(ix) Use initial forensic evidence and perform information security event containment.
(x) Promptly investigate, document, and report Security Incidents in accordance with 1 TAC Chapter 202 and applicable DIR Standards including documenting the incident in the MSI's incident management tool.
(xi) According to the defined process, promptly communicate and escalate security Incidents to DCS Customers, MSI, SCPs, and DIR.
(xii) Oversee and direct SCPs as they conduct information security RCAs, and, if necessary, develop and implement formal Corrective Actions or remediation plans once approved by DIR and the appropriate DCS Customer Assist the MSI and SCPs as they conduct RCAs, and, if necessary, assist in the development of formal Corrective Actions or remediation plans.
(xiii) Evaluate the analysis and proposed Corrective Actions to ensure future risks are adequately mitigated.
(xiv) Provide for security evaluations of security Incidents.
(xv) Provide Incident investigation support.

### 3.10.1. Multi-SCP Incident Resolution

To the extent any incident or problem is due to errors or defects within an in-scope Service environment, supported element or in-scope element licensed or provided by a third party to any DCS Customer, the Successful Respondent, in alignment with the MSI, shall:

(i) Assist the DCS Customer by referring such incident to the appropriate third-party vendor for resolution and coordinating with the third-party vendor as appropriate;
(ii) Perform trend analyses at the DCS Customer's request, and no less frequently on a quarterly basis when not otherwise requested, on the volume and nature of incidents in order to identify possible areas for improvement within DCS; and
(iii) Implement measures to help avoid unnecessary recurrence of incidents, by performing root cause analysis and event correlation.

## 3.11. Risk Management and Tracking

(a) The Successful Respondent shall support the MSI-led Risk Management program and provide Security Risk Management and Tracking related to the environment and services within the context of the Security Operations Services. The goal of Risk Management includes quantifying the impact to the business, determining the likelihood of a threat or vulnerability occurrence, and notification of the MSI, SCPs, DIR, and/or Customers via a DIR agreed upon method.

(b) The Successful Respondent shall, at a minimum:

- (i) In support of DIR and MSI-led business risk management, participate in and contribute to the Risk Management process to identify, analyze, quantify, manage and reduce security risks in the DIR Shared Services environment.
- (ii) Participate in on-going Security Risk Management and assessment activities in coordination with the MSI, DIR and Service Component Providers.

(c) To support the Risk Management Program, the Security Risk Management program manager is responsible for executing the following in support of the Security Operations Services:

- (i) Analyze and document information related to threats, vulnerabilities, and risks.
- (ii) Participate in an annual risk summit with DIR, the MSI, and SCPs to perform a comprehensive review of security risks, treatment plans and identify further remediating actions.
- (iii) Develop, maintain, and provide ongoing oversight of the Security Risk Management portfolio of prevention and treatment plans, initiatives and risk reduction projects.
- (iv) Monitor execution of new and existing risk prevention and treatment plans.
- (v) On a periodic basis as agreed to by the MSI and DIR, report on progress in security risk reduction projects.
- (vi) Track and generate Security Risk Management Program reporting on a monthly basis including prevention and treatment plan actions with status, and risk reduction measures as required by DIR.
- (vii) Under DIR's direction, improve the Security Risk Management process as required.
- (viii) Ensure integration with the MSI Risk Management program to ensure significant risks to the enterprise are reported to executive management.

(d) A security representative shall participate in the MSI's annual facilitated risk session and are responsible for the following:

- (i) Actively participate in sessions for threat, vulnerability, and risk identification.
- (ii) Consult with Successful Respondent teams and providing insight on threats and vulnerabilities relevant to Successful Respondent's scope of work.
- (iii) Identify and provide feedback on potential mitigation and management approaches.
- (iv) Contribute to the review of the Risk Management description, strategy, plan and initiatives.

(e) Support the Security Risk Management planning activities of DIR and DCS Customers in regard to the Services and IT environment.

## 3.12. Steady State Security Operations, Maintenance and Monitoring Requirements

### 3.12.1. Routine Maintenance, Patching, Updates and Hot-Fixes

The Successful Respondent will in consultation and agreement with the State establish, publish and follow a schedule and process for performing routine maintenance, patching, updates and hot-fixes to the Services within its scope. As part of these Services the Successful Respondent will:

(i) Assess, develop, and recommend opportunities to reduce (or avoid) costs associated with support and operations;

(ii) Monitor OEM software and hardware recommended or required configurations, patches, updates, hotfixes and upgrades for all elements that are utilized in the DCS security environment, and prior to any production deployment, ensure that such items are understood, follow OEM guidance and requirements, and are tested in a non-production or laboratory environment prior to their introduction to DCS;

(iii) Provide appropriate Successful Respondent-related data for periodic DIR analysis and review of resources deployed for preventive maintenance and planning preventive maintenance;

(iv) Monitor and analyze trends to identify potential issues and follow-up on recurring problems;

(v) Maintain systems in accordance with DIR strategies, principles, and standards relating to technical, data and security standards as agreed-upon in this Exhibit, Projects, or the SMM or other supporting documents;

(vi) Install systems software upgrades and enhancements for updates or revisions (i.e., 1.x, where x is the update/revision) as necessary to maintain the operability of the Services and implement technology changes (e.g., Systems software upgrades or new scheduling software);

(vii) Included in the scope of such adaptive development work is testing new interfaces to DCS Customers, customer environments and systems, public cloud providers and external customer trading partners that utilize DCS security services;

(viii) The Successful Respondent will install any major systems software upgrades and enhancement for versions (i.e. N.1, where N is the version) as a Project approved by DIR;

(ix) Coordinate with designated State production staff, to manage production schedules;

(x) Update access and parameter or environment configurations contained within in-scope environments, where applicable;

(xi) Establish a production calendar inclusive of daily and periodic maintenance activities;

(xii) Generate and provide access to the DIR to daily production control and scheduling reports, including the production of monthly summary reports that track the progress of the Successful Respondent's performance of maintenance work;

(xiii) Provide timely responses to DIR, DCS Customer, and MSI requests for information and reports necessary to provide updates to business units and stakeholders;

(xiv) Monitor operations for correctness and adherence to agreed quality, performance and availability criteria as set forth in mutually agreed to Operations manuals, associated policies and procedures or other supporting documents as required;

(xv) Support production staff (both DIR and Successful Respondent) to create and adapt IT operational processes and procedures related to the in-scope environments; and

(xvi) Ensure that all system software, bios/microcode, updates, patches and hot fixes are inventoried, cataloged, backed up and available to any service element both prior to any maintenance activity and following the successful deployment to the DCS security environment.

### 3.12.2. Level 2 and 3 Support Services

(a) The MSI Service Desk will provide the Single Point of Contact (SPOC) for day-to-day communications between the State key personnel/IT staff and Application Administrators and end-users. Requests and incidents are reported by Users to the State Business and IT organizations through the MSI Service Desk in accordance with the SMM Service Operations manual or other supporting documents. It is the single contact point for the DCS Customers to record their DCS problems and requests related to the supported servers and the Applications on those supported servers. If there is a direct solution that pertains to State policy, process, procedures, implemented system functions, user support questions, and common solutions. The MSI Service Desk will provide immediate resolution if possible, otherwise it will create an incident report which, depending on the nature of the issue, may require the support of the Successful Respondent for resolution.

(b) Incidents will initiate the appropriate chain of processes: Incident Management, Problem Management, Change Management, Release Management and Configuration Management. This chain of processes will be tracked using the State's trouble ticketing system, which records the execution of each process, quality control point, and store the associated output documents for traceability.

(c) The following classification responsibility matrix shall be utilized by the State and Successful Respondent in consideration of level 2 and level 3 help desk services:

**Table 4: Classification Responsibility Matrix**

| Help Desk Level / Support Tier | Representative Functions | Responsibility |
|---|---|---|
| **Level 0** | Customer "Self Help": routine password resets, common issues, FAQ, Job-Aids etc. | **End-User** |
| **Level 1** | State Specific, routine, Policy, Process, Procedure, Routine Business or Transactional Processing matters that require user support, but no input or support from the Successful Respondent | **MSI** |
| **Level 2: Service Issues** | State Specific, complex Policy, Process, Procedure, Routine Business or Transactional Processing matters that require user support, but advisory or consultative support from the Successful Respondent, but nonetheless do not require remediation (e.g., code, configuration or alteration to the State operational software base) | **MSI,** limited/advisory support of Successful Respondent |
| **Level 2: Security or Solution Issues** | Those issues arising from the aforementioned levels that require the direct involvement of the Successful Respondent due to their complexity and potential impacts to code, configuration, job schedules, interfaces and/or reports | **Successful Respondent**, with MSI and Customer Support |

| Help Desk Level / Support Tier | Representative Functions | Responsibility |
|---|---|---|
| **Level 3: Security / Solution Issues, all Severity 1 or 2 Defects or Outages** | Those issues arising from the aforementioned levels that require the direct involvement of the Successful Respondent due to their complexity and potential impacts to code, configuration, job schedules, interfaces and/or reports.<br>Issues involving any combination of Successful Respondent Provided Software, State Infrastructure and/or 3rd Party Elements (e.g., databases, operating systems, job schedulers, integration software) | **Successful Respondent**, with MSI, Customer and OEM Support (as applicable) |

(d) For each incident escalated to the Successful Respondent by DIR that DIR cannot resolve without the involvement of the Successful Respondent, the Successful Respondent will:

(i) Handle incidents and requests through full life cycle management of all service requests as set forth in the SMM or other supporting operational documents;
(ii) Provide a SPOC for entry and exit to the service process and providing an interface for 3rd Parties essential to the service processes;
(iii) Provide ease of use and a good customer experience for DCS Customers;
(iv) Maintain security and assuring data integrity as required for the successful operation and maintenance of the system; and
(v) Provide timely and effective communication which keeps the State Business and IT Users informed of progress and of appropriate advice on workarounds.

(e) Successful Respondent responsibilities further include:

(i) To the extent incidents cannot be resolved by the centralized State service desk, tracking, monitoring, responding to requests and incidents and resolving incidents consistent with the established operational baselines and referring, as set forth in a SMM or other supporting documents, requests to break/fix support resources for additional assistance;
(ii) Providing documentation for the Successful Respondent's development of or modifications to the Service Desk to help minimize transfers to specialized support;
(iii) Providing the State with an updated list of Successful Respondent-provided Level 2 Support personnel or "on call" personnel who are responsible for Level 3 software support, including contact phone numbers; and
(iv) Working to correct environment defects or problems that require environment code or operational modifications in keeping with Service Level Requirements.

### 3.12.3. Emergency Break / Fix Support

(a) In the case of a State declared emergency, an active security threat or Severity 1 or 2 outage, and in keeping with State security policies in effect, the Successful Respondent may make temporary Emergency System Environment Changes at any time and without State approval should it be unavailable to the Successful Respondent, to the extent such System Changes are necessary, in the Successful Respondent's judgment,

(i) to maintain the continuity of the Services;
(ii) to correct an event or occurrence that would substantially prevent, hinder or delay the operation of State critical business functions; and

(iii) to prevent damage to the State's infrastructure.

(b) The Successful Respondent will promptly notify the State of all such temporary System Environment Changes. At the conclusion of the emergency the Successful Respondent will restore any System Environment Changes to the pre-emergency state, and if the change is deemed necessary for normal operation of the system, a corresponding change request will be initiated for State review and approval.

### 3.12.4. Operations Reporting

(a) The Successful Respondent must provide an automated data feed as defined by the MSI to provide for MSI generation of infrastructure-level operations reporting services for all in-scope service elements and environments that include:

(i) Providing the MSI with data required for summary reports tracking the progress of the Successful Respondent's performance of maintenance work as well as access to daily reports to confirm progress against agreed upon operational and maintenance calendars.

(ii) Timely responses to the DCS Customer requests for information and reports necessary to provide updates to DCS Customer business units and stakeholder constituencies.

(iii) For production or DCS Customer-impacting issues that result in a down system, or the unavailability of a production component, the Successful Respondent must report progress until the issue is corrected and/or the DCS Customer agrees that the issue causing the unavailability situation has been corrected. In all cases, the minimum reporting standard will be dictated by the SLA for the impacted service.

(b) The Successful Respondent shall:

(i) Perform activities required for monitoring and optimizing performance in order to reduce costs or improve Service Levels.

(ii) Provide performance monitoring, tuning, and reporting, including remote monitoring where applicable.

A. Provide Authorized Users with access to real-time system monitoring information via the MSI portal.

B. Provide guidance for active prevention of Service performance events (e.g., file Central Processing Unit (CPU), file system level storage, memory, server network interface throughput).

C. Monitor and alert on thresholds (e.g., dataset or table space capacity events, full log files, file systems, etc.), and provide alerts to DCS Customers as specified in the SMM.

D. Provide systems performance reviews and advice.

(iii) Perform upgrades to optimize capacity, manage to established thresholds, exceed Service Levels and meet Software architectural requirements.

(iv) Coordinate with the business partners, Third Party Vendors, other SCPs, DIR, and DCS Customers as appropriate on projects to install/upgrade hardware and software.

(v) Provide and install necessary tools to perform monitoring and reporting.

(vi) Provide status and trending reports as required, including:

A. reports to highlight production incidents and problems and establish predetermined action and escalation procedures when batch window incidents and problems are encountered.
B. report to DIR and DCS Customers on resource shortages, and report utilization statistics and trends to DIR and DCS Customers on a monthly basis at a level of detail sufficient to identify exceptions.

(vii) Monitor Applications as required to proactively prevent or resolve Application performance, degradation or failure where such activities are part of the Service.
(viii) Monitor data storage media and processor utilization and requirements.
(ix) Provide Managed System Performance Monitoring service to support proactive and persistent monitoring of critical enterprise applications.

### 3.12.5. Security Operations Support

(a) The Successful Respondent must provide operations support services for all in-scope DCS environments, that specifically include:

(i) Implementing and monitoring the security environment management services operations;
(ii) Monitoring security environment operations for correctness and adherence to agreed quality, performance and availability criteria;
(iii) Supporting DCS Customer and SCP production staff to create and adapt IT operational processes and procedures related to the in-scope DCS environments and standards;
(iv) Communicating appropriately with the DCS Customer designees, Service Component Providers, authorized users and third-party vendors;
(v) Performing in-scope ad hoc operations reporting as directed by DIR;
(vi) Providing support functions during a crisis;
(vii) Serving as primary point of contact and leading IT security operations support for the in-scope DCS environments; and
(viii) Acting as a resource with respect to knowledge and information sharing regarding the supported security environment, as required by DCS Customers, DCS SCPs and DIR.

(b) This must include providing information and consulting support with respect to: service performance, providing assistance with infrastructure security integration and operations testing, debugging and remediation of security issues and vulnerabilities, designing appropriate test environments, performing training, and maintaining system documentation.

### 3.12.6. Security Solution and Operations Reporting

The Successful Respondent must provide DCS infrastructure level security operations reporting Services for all in-scope environments that include:

(i) Timely responses to the DCS Customer requests for information and reports necessary to provide updates to DCS Customer business units and stakeholder constituencies.
(ii) For production or customer impacting issues that result in a down system, or the unavailability of a production component, the Successful Respondent must report progress based on the service level agreement until the issue is corrected and/or the

DCS Customer agrees the issue causing the unavailability situation has been corrected. In all cases, the minimum reporting standard will be dictated by the service level agreement for the impacted service.

### 3.12.7. Ad-Hoc Request Support Obligations

(a) Generally, Ad-Hoc requests are infrequent in nature, and will require the Successful Respondent to fulfill or assist with and will be specific to the scope of the work contracted. The Successful Respondent must support Ad-hoc requests for all in-scope DCS environments, under the following considerations:

(i) Requests within the Successful Respondent scope of work that requires Successful Respondent involvement to fulfill or assist with;
(ii) Ad-hoc requests require no modification, configuration, customization or system testing of the environments;
(iii) Requests will normally be made through the DCS Level 1 (MSI) service management platform to effectively track and manage demand; and
(iv) Routine tracking procedures will provide visibility of all ad-hoc requests.

(b) Examples of ad-hoc requests may include, but not be limited to:

(i) Participation in service review meetings with specific Agencies or on a sub-set of a meeting where Successful Respondent expertise may be valuable to DIR;
(ii) Assisting the State in troubleshooting an application issue where the root cause is difficult to determine as an infrastructure or application issue (e.g., intermittent connectivity issue, failing storage device, re-boot of an application server);
(iii) Generation of an ad-hoc report based on in-scope data (e.g., asset inventory, help desk call volume) to support State decision making; and
(iv) Supporting the State in prospective conversations or capability demonstrations as part of DCS outreach and growth with DCS Prospects that are not currently in the service to migrate to using DCS.

### 3.12.8. Security Systems Management and Administration

The Successful Respondent must provide Systems Management and Administration Services for all in-scope Service elements:

(i) Coordinating the installation, testing, operating, troubleshooting and maintaining of the security system(s), configuration items, hardware, software, appliances and other elements that comprise the Service;
(ii) Identifying, testing, packaging patches and other updates associated with supported operating system(s), configuration items, hardware, software, appliances and other elements that comprise the Service, as well as supporting additional security-related fixes associated with the operating system(s), configuration items, hardware, software, appliances and other elements that comprise the Service;
(iii) Managing the security functions related to the operating system(s), configuration items, hardware, software, appliances and other elements that comprise the Service including administrative access and passwords and the related security controls to

maintain the integrity of the operating system, based on State standard security processes;

(iv) Supporting security and infrastructure protection solutions for the systems that are being managed by the State;

(v) Ensuring that, unless otherwise requested by the State under an approved exception request, solution delivery elements including but not limited to: software, microcode, patches, operating systems, connectivity software are maintained in accordance with the State policies in effect at the time and have a currency level no older than current major release (N) or immediate prior major release (N-1), and in all cases are supported by the 3rd party software or hardware vendor;

(vi) The Successful Respondent must strive to accommodate the DCS Customer testing, review and approval processes prior to the installation of these elements in a production environment; and

(vii) Backup and system restore of all applicable Service software, configuration(s) and data.

## 3.13. Cybersecurity Assessment

(a) The State requires an annual Cybersecurity Assessment be performed for the DCS Program as a whole and of the DCS SCPs. At DIR's sole discretion this Cybersecurity Assessment of the Security Program may be conducted by the Successful Respondent, DIR or, a third-party security assessment SCP (the "Security Assessment Company") through the Managed Security Services program. The assessment will address strengths, challenges, opportunities and direction with regard to protecting the State enterprise from Cyber threats. The assessment will serve as input to continuous improvement of DCS security.

(b) The Successful Respondent will action the Cybersecurity Assessment output and lead mitigations across the MSI, SCPs and Customers for DCS services findings.

(c) The Successful Respondent will use the Cybersecurity Assessment output as input to perform a fit/gap analysis using State capabilities and industry best practices to identify a multi-year strategy and plan to enhance the State's capabilities in response to ongoing evolutions in the Cyber-threat detection, mitigation and response.

### 3.13.1. Cybersecurity Assessment Performed by Respondent

If DIR requests to have the Successful Respondent perform a Cybersecurity Assessment through the RFS process, the Successful Respondent shall:

#### 3.13.1.1. Assessment Procedures

The Successful Respondent shall, at a minimum:

(i) Meet with DIR, the MSI, and/or the Security Assessment Company, as applicable, for the purpose of agreeing upon a detailed plan (including time deadlines for provision of data by all SCPs and the Successful Respondent) for conducting and completing each Assessment.

(ii) The Successful Respondent or the Security Assessment Company, as applicable, will "normalize" all data to obtain relevant comparisons for purposes of each Assessment in accordance with DIR's and the State's then-current practices and methodologies.

(iii) Cooperate fully with DIR and/or the Security Assessment Company and provide reasonable access to any premises, equipment, personnel or documents and provide any assistance required by DIR and/or the Security Assessment Company to conduct the Assessment, at the Successful Respondent's cost and expense; provided, however, DIR and the Security Assessment Company shall not have access to Successful Respondent's proprietary information where it is not relevant to the Assessment, and shall further not have access to confidential or proprietary information of Successful Respondent customers other than DCS Customers.

(iv) Under no circumstances will Successful Respondent attempt to persuade or control or otherwise influence the Security Assessment Company in the determination of its findings. The Assessment shall be conducted so as not to unreasonably disrupt Successful Respondent's operations under this Agreement.

(v) Within fifteen (15) days of an Assessment Notice Date, DIR, the Successful Respondent, MSI, and all SCPs will meet to jointly review the relevant Assessment report and if such report concludes that the Security Program does not meet or exceed the Standard of Due Care, then within thirty (30) days after the applicable Assessment Notice Date, the affected SCPs and the Successful Respondent shall develop and agree upon an action plan to promptly address and resolve any deficiencies, vulnerabilities, concerns and/or recommendations identified in such report, consistent with the affected SCP's (or the Successful Respondent's) obligations as set forth in the Agreement.

(vi) The Successful Respondent, in support of the MSI, will ensure the affected SCP shall, within six (6) months after the applicable Assessment Notice Date, complete all remedial action in accordance with such action plan in order to resolve such deficiencies, vulnerabilities, and concerns and implement such recommendations.

(vii) DIR will receive Deliverable Credits pursuant to Exhibit 3.1 Service Levels Matrix and Exhibit 3.3 Critical Deliverables should the Successful Respondent or an SCP fail to take remedial action in accordance with such action plan.

#### 3.13.1.2. Assessment Metrics

(a) The Successful Respondent will be apprised of the metrics sufficiently in advance of each Assessment to establish administrative processes to capture the necessary metric data.

(b) The exact metrics to be included in an Assessment will be contingent upon (1) the detail in which the Security Assessment Company maintains security data within its database and (2) Successful Respondent's ability to capture security information at the desired level of detail.

(c) DIR and the Security Assessment Company will use the then-current NIST, ISO 27001/27002, the Texas Cybersecurity Framework, and TAC Section 202 frameworks, where applicable, to conduct Assessments.

#### 3.13.1.3. Analysis Phase

(a) Based on the above, the Successful Respondent will perform a detailed analysis of the information gathered and develop a fit/gap analysis (again, using the TAC 202, NIST, and COBIT 5 Frameworks) between current capabilities, strengths, weaknesses, opportunities and threats across the following three (3) dimensions:

(i) people/organization;
(ii) policy/processes; and
(iii) technology and tools.

(b) The Successful Respondent, as part of the work, will develop a **DCS-specific** analysis that includes fact based observations, issues/risks and tactical/strategic issues facing the State using frameworks, augmented with industry best/leading practices as well as Successful Respondent specific methods and approaches to identifying the challenges and mitigants facing the State's implementation of Cybersecurity.

(c) During this phase, the Successful Respondent will assess operating dependencies and support processes between State Security, Customer DCS Operational personnel, and DCS infrastructure Service Component Providers (e.g., network, server/storage, print/mail, mainframe, cloud) to develop a complete view of the operating environment pertaining to Cybersecurity in DCS. Pending the ongoing needs of DCS Customers, and subject to the successful performance of the Successful Respondent, the State may elect to authorize additional work under a mutually agreeable Service Request on an enterprise or agency specific basis to the Successful Respondent arising from this solicitation for similar and related projects.

### 3.13.2. Recommendation / Planning Phase

(a) Based on the Cybersecurity Assessment output, the Successful Respondent will collaborate with DIR to develop an actionable set of recommendations for the State to consider implementing, again across the three broad categories of people/organization, policy/process and tools/methods as well as general implementation approaches inclusive of timing, dependencies, support and cost requirements. Upon State approval of these recommendations, the Successful Respondent will develop an actionable and realistic implementation plan working with the MSI, SCPs and DCS Customers as needed to address gaps identified.

(b) The State Annual Cybersecurity Assessment Deliverable criteria is described in **Attachment 1.1 Deliverables**.

## 3.14. Disaster Recovery Support Services

(a) Based on the current capabilities of the State, the overall complexity of the State's computing applications and services portfolio, and existing customer provisions for disaster recovery and business continuity (DR/BC), the responsibilities shall in general: i) apply to in-scope service elements; ii) the all service elements as required to continuously operate and provide the Service itself in consideration of then current capabilities and responsibilities.

(b) The Successful Respondent's responsibilities with respect to the DR/BC services must include the following:

(i) The Successful Respondent must support business continuity plans as they relate to in-scope Service elements and participate in and demonstrate regular testing and improvement of the business continuity plans as required to provide the Service;

(ii) To the extent agreed appropriate, allow DIR upon request to participate in planning sessions, testing review sessions and other meeting activities as necessary to validate the efficacy and merits of the Successful Respondent DR/BC plan to provide the Service elements in the event of a disaster;

(iii) Support the State's potential future specification, design and implementation of Service disaster recovery plans for in-scope service elements as agreed based upon the following principles:

A. Leverage an offsite and geographically diverse alternate disaster recovery site that has sufficient computing and network capabilities which are adequate to provide the Service during an outage period.

B. Document requirements and support design reviews to facilitate transfer of Service operations to disaster site within forty-eight (48) hours of failure of the primary site

C. Document procedures to restore primary Service operations (once available) within twenty-four (24) hours.

D. Specification of redundant service requirements (security devices and telecommunications access) to ensure 24x7 operations for State critical Service components.

### 3.14.1. Disaster Recovery Overview and General Requirements

(a) The State MSI leads, manages, and oversees the Disaster Recovery Program (DRP) within DCS including Planning and Testing activities. Based on the current capabilities within DCS, the overall complexity of DCS Customer computing applications and services portfolio, and existing DCS Customer and TSS SCP provisions for disaster recovery and business continuity (DR/BC), the scope and responsibilities of the Successful Respondent are as follows:

(i) DR will apply to in-scope service elements located in the DIR Facilities including the facility itself in consideration of existing capabilities and, following implementation, Successful Respondent Services to DIR;

(ii) DR will apply to in-scope service elements located in non-consolidated facilities (legacy data centers and remote business offices);

(iii) Does not apply to existing co-location Customers;

(iv) DR will apply to any Service elements that are under the scope and responsibility of the Successful Respondent in delivery of Services to Customers who elect to consume DR from the DCS program via the Successful Respondent;

(v) DR will apply to all Successful Respondent services and Service support infrastructure elements as required to operate and maintain the Services including all infrastructure and operational elements that the Successful Respondent provides or is dependent upon to deliver the Service to DCS Customers and, as applicable, other DCS SCPs;

(vi) The Successful Respondent will ensure that any existing implemented DR methods to enable specified DR/BC for DCS Customer applications and systems are not diminished as a result of Successful Respondent efforts;

(vii) Be designed and implemented to complement DCS Customer activities in support of the DCS Customer's overall DR and business continuity plan(s);

(viii) DR will apply to successful system state restoration including recovery of application environment and associated data. DR does not apply to middleware and application software configuration, application presentation, customizations or extensions, and is limited to in-scope environment elements unless otherwise agreed to with DIR or DCS Customer;

(ix) Except as otherwise provided, DCS Customers will retain sole responsibility for overall business continuity plans. The Successful Respondent retains responsibility for business continuity plans for in-scope services and facilities;

(x) Enable DCS Customer and TSS SCP activities, processes and procedures for in-scope work and environments to deliver DCS Customer disaster recovery capabilities; and

(xi) Provide input into DIR's potential future specification, design and implementation of infrastructure disaster recovery plans for in-scope environments and environment elements, but exclusive of middleware, application or presentation software as agreed based upon the following principles:

A. Leverage the alternate CDC facility (Austin -> San Angelo or San Angelo -> Austin) or one (1) or more location of the Successful Respondent in the event of a disaster in one of the data centers. The existing CDCs are designed and must be supported to serve as a geographically diverse alternate disaster recovery site that has sufficient computing and network capabilities which are adequate to process the DCS Customers' and TSS SCP operations and to provide systems access to end-user personnel during an outage period.

B. Document requirements and participate in design reviews to facilitate transfer of operations to disaster site for in-scope environment elements to occur within forty-eight (48) hours of failure of primary site.

C. Document procedures to restore primary operations for in-scope environment site operations (once available) within twenty-four (24) hours.

D. Identification of redundant processing environment requirements to ensure 24x7 operations for DCS Customer-critical infrastructure components.

E. Specification of redundant power requirements to ensure 24x7 operations for DCS Customer-critical infrastructure components.

F. Specification of redundant networking requirements (network devices and telecommunications access) to ensure 24X7 operations for DCS Customer-critical infrastructure components.

(b) The following table is a summary of the scope and responsibilities of DR services:

**Table 5: Summary of Required Disaster Recovery Services**

| DR Scope Area | Key Elements | Successful Respondent | DCS Customer | MSI |
|---|---|---|---|---|
| **Overall DR Planning and Testing (DCS Program)** | DCS Program-level planning and coordination Services<br>DCS Program Reporting<br>DCS Program DR Enhancement / Optimization planning | Participate | Participate | Lead |
| **DR Service Implementation** | Design and Implementation of DR Services for DCS Customer Environments<br>DR Implementation testing / validation<br>Remediation of any detected DR defects or issues<br>DR Operations | Participate as needed | Validate | Informed |
| **Computing Elements** | As provided to: DCS Customers; any DCS SCP using Services contained in this Exhibit; and any DIR shared services Customer or provider upon request.<br>Scope includes both production and non-production (e.g., development, test) elements within the DCS program. | Participate as needed | Consulted<br>Validate | Validate |
| **Service Delivery Infrastructure** | All Successful Respondent provided Service Delivery elements including operational, security, network, monitoring and other elements as included in the Successful Respondent's Service | Participate as needed | - | Informed |

### 3.14.2. Other Disaster Recovery Requirements

### 3.14.3. Security Service DR Testing Responsibilities

The Successful Respondent will:

(i) Develop improvements and (if required) redesign elements of the Service to improve the reliability, availability and utility of the Service with respect to DR testing, failover, load balancing and redundancy.

(ii) Support DCS in establishing joint test objectives with a customer, designed to verify that the in-scope Service elements will be available within the agreed upon timeframes contained in the business continuity plan as they pertain to in-scope Service elements.

(iii) Support DCS in scheduling and testing in scope environment elements of the disaster recovery and business continuity plans relating to in-scope Service elements at least annually, as found in **Attachment 1.1 Deliverables**, in support of the customer, its

designees, any testing and recovery providers, and relevant State third-party service providers.

(iv) Continuing to operate and manage the in-scope Service elements during periodic disaster recovery tests.

### 3.14.4. Security Service DR Communications

(a) The MSI is responsible for all DR coordination and communications. As part of the Service and in support of the MSI and DCS Customers, the Successful Respondent will be responsible for:

(i) Following established MSI procedures to notify impacted customers and DIR as soon as practicable upon becoming aware of a disaster or outage affecting the contracted Services.

(ii) Working with the State to support implementation of a customer disaster recovery and business continuity plan. In such regard, the Successful Respondent will:

A. Perform necessary migrations of the software code and data as defined in the customer disaster recovery plan to reinstate the in-scope environment elements so that they are functional at a backup location designated by a customer in accordance with the established procedures.

B. Coordinate with the customer to support the reinstatement of the in-scope Environment(s) at such backup location for in-scope environments.

C. Maintain provision and ongoing operation of the Services for unaffected areas.

D. Following any disaster, at either DIR's or the customer's request, the Successful Respondent will support DCS and the customer in the reinstallation any in-scope environment elements affected by such disaster in accordance with the process for such re-installation set forth in a disaster recovery plan and business continuity plan.

E. Following any disaster, conducting a post-disaster meeting with the State for the purpose of developing or enhancing plans to mitigate the adverse impact of future occurrences as they relate to in-scope environment elements.

F. To the extent applicable to the in-scope environment elements, maintain compliance with State documented disaster recovery policies, standards, and procedures contained in a provided disaster recovery and business continuity plan.

G. Support an annual test, documented results and feedback procedures contained in the State provided disaster recovery and business continuity plan for in-scope infrastructure environment elements.

(b) The Successful Respondent shall not be responsible for, or quote or specify services associated with development of detailed disaster recovery or business continuity plans for State applications; these plans shall remain the sole responsibility of the DCS Customer that maintains the application.

## 3.15. Reporting

As part of the Service, the Successful Respondent shall:

(i) Generate and provide access to DIR and MSI to daily production control and scheduling reports, including the production of monthly summary reports that track the progress of the Successful Respondent's performance of maintenance work (details are contained in **Appendix A Reports**).

(ii) Provide all current state reports as described in **Appendix A Reports** and required in Articles 6 Performance Model – Service Level Agreements, and 9 Cross-Functional Services.

(iii) Perform in-scope ad hoc operations reporting as directed by DIR.

## 3.16. Compliance

The Successful Respondent shall perform the Services in accordance with the terms of the Contract and DIR's and DCS Customers' then-current policies and procedures until the SMM is finalized and agreed upon by the Parties. Thereafter, the Successful Respondent shall perform the Services in accordance with the terms of the Contract, including the SMM. In the event of a conflict between the provisions of the Contract and the SMM, the provisions of the Contract shall control unless the Parties expressly agree otherwise and have revised the Contract through the appropriate contract change control process.

## 3.17. Quality Assurance

(a) The Successful Respondent will be responsible for adhering to quality assurance processes and procedures developed by the MSI. Successful Respondent should provide documentation related to its approach for ensuring continuous quality assurance processes and procedures for the delivery of Services including:

(i) Confirming compliance with agreed upon quality assurance procedures;

(ii) Conducting quality and progress reviews with appropriate DCS Customer personnel;

(iii) Supporting MSI with developing and publishing a quality assurance/quality control (QA/QC) manual;

(iv) Verifying compliance with the published QA/QC manual;

(v) Maintaining Service equipment and software quality consistent with its obligations; and

(vi) Documenting and implement process improvement including identifying industry leading practices.

(b) Successful Respondent shall develop and implement Quality Assurance and internal control (e.g., financial and accounting controls, organizational controls, input/output controls, system modification controls, processing controls, system design controls and access controls) processes and procedures, including implementing tools and methodologies, to perform the Services in an accurate and timely manner (and confirm that they are so performed and accounted for) in accordance with (1) the Service Levels and other requirements of this Agreement, (2) Generally Accepted Accounting Principles (US GAAP) to the extent necessary for Successful Respondent to make its public filings with the Securities and Exchange Commission, (3) accepted industry standards of first tier providers of services that are the same as or similar to the Services, (4) the Laws applicable to DIR and the DCS Customers (without limiting the obligations of the Parties under **MSA, Section 8.11 Compliance with Laws**, and (5) industry standards (e.g., QS 9000, ISO 9001/2000, ISO 14000, ISO 17799/2005, ISO 27001/2005, ISO 27002/2005) applicable to DIR and the performance of

the Services to the extent described in Section 3.18 Industry Standards, Certifications and Compliance. Such processes, procedures and controls shall include verification, checkpoint reviews, testing, acceptance and other procedures for DIR and the DCS Customers to assure the quality and timeliness of Successful Respondent's performance. Without limiting the generality of the foregoing, Successful Respondent shall:

(i) Maintain a strong control environment in day-to-day operations to assure that the following fundamental control objectives are met:
   A. financial, billing and operational information is valid, timely, complete and accurate;
   B. operations are performed efficiently and achieve effective results, consistent with the requirements of this Agreement;
   C. assets and data are safeguarded in accordance with Successful Respondent's own internal (and in all events reasonable) practices (but without expanding Successful Respondent's obligations under **MSA, Section 6.2.2 Safeguarding of DIR Data**); and
   D. actions and decisions of the organization are in compliance with Laws (without limiting the obligation of the Parties under Section 3.18 Industry Standards, Certifications and Compliance) and the terms of this Agreement;

(ii) Build the following basic control activities into work processes:
   A. accountability clearly defined and understood;
   B. access properly controlled;
   C. adequate supervision;
   D. transactions properly authorized;
   E. transactions properly recorded;
   F. transactions recorded in proper accounting period;
   G. policies, procedures and responsibilities documented;
   H. adequate training and education; and
   I. adequate separation of duties;

(iii) Perform periodic control self-assessments with respect to all Services as necessary to ensure compliance;

(iv) Maintain an internal audit function to sufficiently monitor the processes, internal controls and Systems used to provide the Services (i.e., perform audits, track control measures, communicate status to management, drive corrective action, etc.) and provide copies of any such internal audit reports to DIR upon request; and

(v) Conduct investigations of suspected fraudulent activities within Successful Respondent's organization that impact or reasonably could be expected to impact DIR or the DCS Customers. Successful Respondent shall promptly notify DIR of any such suspected fraudulent activity and a reasonable summary of the results of any such investigation as they relate to DIR or the DCS Customers and such supplemental materials as DIR may reasonably request. At Successful Respondent's request, DIR shall provide reasonable assistance to Successful Respondent in connection with any such investigation.

(c) Successful Respondent shall submit such processes, procedures and controls to DIR for its review, comment, and approval as part of the SMM process and shall use commercially reasonable efforts to finalize such processes, procedures, and controls and obtain DIR's final approval on or before the established due date. Upon DIR's approval, such processes and procedures shall be included in the Service Management Manual. Prior to the approval of such processes and procedures by DIR, Successful Respondent shall adhere strictly to DIR's and the DCS Customers' then-current policies, procedures and controls. No failure or inability of the quality assurance procedures to disclose any errors or problems with the Services shall excuse Successful Respondent's failure to comply with the Service Levels and other terms of this Agreement.

## 3.18. Industry Standards, Certifications and Compliance

Successful Respondent shall comply with TAC 202, PCI, HIPAA, MARS-E, IRS 1075, CJIS, SSA, ISO 9000, ISO 9001:2000, ISO 14001, ISO 27001/2005, and ISO 27002/2005 and shall apply ITIL standards and Six Sigma processes.

### 3.18.1. SOC 2 Reports

(a) In addition to its other obligations under this Section, Successful Respondent shall cause a Service Organization Controls 2 Report, type II, [("SOC 2 Report") (SOC 2: Attestation Standards, Section 101 of the AICPA Codification Standards (AT Section 101), "Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2)", as published by the AICPA in 2011] to be conducted by an independent, nationally recognized public accounting firm qualified to perform such audits at least annually, prepared in accordance with the relevant and current standards. The Successful Respondent acknowledges that each such SOC 2 Report shall cover Successful Respondent's policies, procedures, controls and systems for twelve (12) months of Successful Respondent's performance of the Services, in accordance with the State fiscal year (and each successive twelve (12) month period thereafter unless otherwise agreed to), and in particular those policies, procedures, controls and systems applicable to an audit of Successful Respondent's customers. Prior to initiating any such SOC 2 Report, Successful Respondent shall confer with DIR as to the scope and timing of each SOC 2 Report and shall accommodate DIR's requested modifications (if any) for each such SOC 2 Report to the extent reasonably practicable.

(b) Successful Respondent shall cause its Subcontractors performing the Services to allow SOC 2 Reports on their policies, procedures, controls and systems that complement the SOC 2 Report performed pursuant to clause (1) above, when requested by Successful Respondent, DIR, Customers, Texas State Auditor's Office, and other entities authorized by DIR. If Successful Respondent is unable to cause its Subcontractors to conduct such SOC 2 Reports or chooses to conduct the SOC 2 Reports of such complementary policies, procedures, contracts and systems itself, then Successful Respondent shall engage an independent, nationally recognized public accounting firm to perform such audits of its Subcontractors to ensure that the policies, procedures, controls and systems of the Subcontractor complement those of Successful Respondent. For purposes of this clause (2), the term "complement" shall mean that the policies, procedures, controls and systems of the Subcontractors, when taken as a whole in combination with the policies, procedures, controls and systems of Successful Respondent, represent the entire control environment under this Agreement.

(c) Unless otherwise agreed by the Parties, a copy of the final annual report dated December 31st will be provided by Successful Respondent to DIR and DIR Auditors ten (10) Business Days from the date Successful Respondent receives the final report from the external firm. In all events, each report delivered by such date shall be unqualified and Successful Respondent shall respond to such report in accordance with **MSA, Section 4.11 Audit Rights**. In addition, within ten (10) Business Days of DIR's written request to Successful Respondent, Successful Respondent shall provide a letter to DIR signed by an officer of Successful Respondent certifying that there has been no change in the policies, procedures, controls and systems of Successful Respondent since the date of the most recent SOC 2 Report.

(d) To the extent DIR provides notice and requests that, in addition to the SOC 2 Reports described in clauses (1) and (2) above, Successful Respondent conduct DIR-specific SOC 2 Report, Successful Respondent shall, at DIR's expense, cause such DIR-specific SOC 2 Report to be performed by a nationally recognized public accounting firm qualified to perform such Report; provided, however, that Successful Respondent timely notifies DIR of such expense, obtains DIR's prior written approval and uses commercially reasonable efforts to minimize such expense. A copy of the final report of each such DIR-specific SOC 2 Report shall be delivered to DIR by Successful Respondent ten (10) Business Days from the date Successful Respondent receives the final audit report from the external firm. If Successful Respondent undertakes additional or different SOC 2 Reports (other than customer-specific audits requested and paid for by other Successful Respondent customers), Successful Respondent shall accord DIR the rights described in clause (1) above with respect to such reports. To the extent DIR provides notice and requests that, in addition to the SOC 2 Reports described in clauses (1) and (2) above, DIR may, in coordination with the DIR Auditors, conduct DIR-specific SOC 2 Report on the services facility at or from which the Services are provided.

(e) During the period when SOC 2 Reports are performed under this Section, Successful Respondent shall provide DIR with periodic updates on the status of such reports and any issues that are specific to DIR or that are reasonably anticipated to impact in any material respect the control environment under this Agreement. Upon completion of any such SOC 2 Report that identifies any significant deficiency or material weakness, Successful Respondent shall prepare and implement a corrective action plan to correct any such deficiency or resolve any problem identified from such SOC 2 Report specific to DIR or that impact in any material respect the control environment under this Agreement. A copy of the corrective action plan shall be provided to DIR within thirty (30) days following the discovery of such deficiency or problem. If the SOC 2 Report shows a control issue that is specific to DIR or that impacts in any material respect the control environment under this Agreement (a "Control Deficiency") that has not theretofore been corrected or properly mitigated and such failure to mitigate the Control Deficiency leads to a qualified opinion being issued by Successful Respondent's auditor, then Successful Respondent's failure to promptly remedy the Control Deficiency will be deemed a material breach of this Agreement triggering a termination rights for DIR under **MSA, Section 13.1 Termination for Cause**.

(f) If Successful Respondent is unable to timely deliver to DIR any report described in this Section that does not identify any significant deficiency or material weakness, Successful Respondent shall:

(i) provide a certificate from an officer of Successful Respondent to DIR certifying, on the date such report is delivered, or is otherwise due to be delivered, the circumstances giving rise to any delay in delivering such report;
(ii) promptly take such actions as deemed necessary by DIR to resolve such circumstances and deliver such report as promptly as practicable thereafter; and
(iii) permit DIR and the DIR Auditors (or their agents), at Successful Respondents' expense, to perform such procedures and testing of the operating effectiveness of Successful Respondent's policies, procedures, controls and systems for the period otherwise covered by such report.

### 3.18.2. Audit Requirements

(a) DIR, DCS Customers, Texas State Auditor's Office, and other entities authorized by DIR may conduct security reviews, assessments, forensic analysis and/or audits (e.g., SSAE 18, State Audit Office, IRS audits) where service is being provided by the Successful Respondent. These assessments may include (but are not limited to) physical security, logical security, policies and procedures, network analysis, vulnerability scans and Controlled Penetration Tests. The Successful Respondent shall cooperate with audits DIR requires.
(b) Successful Respondent shall provide corporate security policies in addition to DCS security policies if required for an audit.

## 3.19. Obligation to Evolve

(a) Successful Respondent shall identify and propose the implementation of Technology Evolutions that are likely to:
(i) improve the efficiency and effectiveness of the Services (including cost savings);
(ii) improve the efficiency and effectiveness of the processes, services and related functions performed by or for DIR and the DCS Customers;
(iii) result in cost savings or revenue increases to DIR and the DCS Customers in areas of their operations outside the Services; and
(iv) enhance the ability of DIR and the DCS Customers to conduct their operations and serve their constituencies and customers faster and/or more efficiently than the then-current strategies. Successful Respondent will cause the Services, Software and other assets used to deliver the Services, as approved by DIR, to evolve and to be modified, enhanced, supplemented and replaced as necessary for the Services, Software, and other assets used to deliver the Services to keep current with industry best practices and a level of technology that is:
A. compliant with all Laws applicable to the provision and receipt of the Services;
B. used by Successful Respondent and other top-tier IT providers in providing services similar to the Services to other customers; and
C. in general use within the IT industry.

(b) Any changes to the Services, Software, and other assets used to deliver the Services implemented in accordance with this Section will be deemed to be included within the scope of the Services to the same extent and in the same manner as if expressly described in this Agreement, at no additional charge to DIR.

### 3.19.1. Flexibility

The technologies and process strategies Successful Respondent employs to provide the Services shall meet industry standards and shall be flexible enough to allow integration with new technologies or processes, or significant changes in DIR's or a DCS Customer's objectives and strategies. For example, Equipment must have sufficient scalability and be sufficiently modular to allow integration of new technologies without the need to replace whole, or significant parts of, systems or processes (e.g. made to be a one-to-many model) to enable DIR's and/or the DCS Customers' operations to become more scalable and flexible.

### 3.19.2. Obligation to Identify Best Practices

Throughout the Term, Successful Respondent shall:

(i) identify and apply best practice techniques, methods and technologies in the performance of the Services;
(ii) train Successful Respondent Personnel in the use of new techniques, methods, and technologies that are in general use within Successful Respondent's organization and the IT and business consulting industries; and
(iii) make necessary investments to keep and maintain the Software and other assets used to deliver the Services at the level of currency defined in this Section.

### 3.19.3. Successful Respondent Briefings

Successful Respondent will meet with DIR at least once during every 180-day period throughout the Term to inform DIR of:

(i) any investments, modifications, enhancements, and improvements that Successful Respondent is required or proposes to make to the Services, Software, and other assets used to deliver the Services pursuant to this Section;
(ii) new information processing technology or business processes Successful Respondent is developing;
(iii) any pending or actual changes in Law that could reasonably be expected to affect the provision or receipt of the Services; and
(iv) technology or process trends and directions of which Successful Respondent is otherwise aware that could reasonably be expected to have an impact on DIR's IT operations or business.

## 3.20. Operating Agreements with Other SCPs and MSI

(a) DIR holds other contracts for additional or related work for the DCS SCPs, platforms and customer specific projects and services. The Successful Respondent must fully cooperate with the MSI and all other DCS SCPs as may be required for the smooth and efficient operation of all related or additional work arising from this Exhibit. The Successful Respondent may not act in any way that may unreasonably interfere with the work of any other DCS participant or DIR or DCS Customers' employees. Additionally, the Successful Respondent must include the obligations of this provision in all its contracts with its subcontractors that work on any Project or Service arising from this Exhibit.

(b) DIR believes that mutually supportive relationships among DCS SCP, in addition to relationships with DIR and the MSI, are required to deliver a seamless and well managed service to DCS Customers.

(c) The Successful Respondent is required to enter into Operating Agreements (OAs) with the MSI and SCP including but not limited to mainframe, print/mail, public cloud, network, and technology solution services, and future SCPs should DIR identify them to the Successful Respondent. The Successful Respondent will contribute to the design of these OAs, and will be responsible for implementing, following and responding to these agreements once developed. At a minimum, these OAs will include SCP to SCP agreements that address processes, protocols and communications for:

(i) Joint operation, issue resolution, and governance of the delivery of Services;
(ii) Customer support functions for multi-service provider solution requests;
(iii) Incidents resolution and project management for multi-service provider escalations;
(iv) Operations management;
(v) Security matters including active or persistent threats and multi-party response/remediation functions;
(vi) The Successful Respondent and the MSI and SCPs will acknowledge and agree in the OA that the Successful Respondent will assist and coordinate the delivery of Services to DIR and DCS Customers. In addition, the Successful Respondent, MSI and SCPs shall each promptly disclose to the other any material difficulties or delays that either experiences in connection with the delivery or operation of the Services;
(vii) Ensuring consistent levels of quality in the DCS environment while providing transparency across all levels of the DCS Service Component Provider organization, to DCS Customers, the MSI and DIR;
(viii) Defined and agreed standards of accountability for all involved;
(ix) Documented interdependencies among SCPs for service delivery, including timing, quality and communications standards as to ensure that handoffs or support requirements between the parties are understood, documented, and followed by all parties;
(x) Service terms, conditions, operating hours, response times, and escalations; and
(xi) Periodic review and optimization of the OAs based on better practices, lessons learned and DCS Customer feedback. The project team leaders from the Successful Respondent, MSI, and SCPs shall meet regularly, but no less frequently than monthly, during the term of this Agreement, to prioritize tasks, discuss changes and scheduling, identify problems and resolutions, and otherwise coordinate and cooperate in connection with the development and implementation of the Services.

(d) Further, the Successful Respondent will establish Operating Agreements (OA) with both other DCS Service Component Providers and the MSI that the Successful Respondent provides services to, or consumes services from in the overall context of the DCS program as to:

(i) Provide a holistic Service to DCS Customers inclusive of all work, process, communication, and data/report sharing requirements contained herein;
(ii) Minimize, and to the greatest extent possible, eliminate process and communication gaps or overlaps in Service Request management, ITIL I/P/C processes, and Service

Delivery processes as to drive a cohesive and well-run Service to DCS Customers and DIR; and

(iii) Ensure participation and success of multi-service provider projects, initiatives, incident and problem resolution within the DCS program where such elements require multi-party participation to deliver a project, resolve an issue or problem, or provide a superior delivery/resolution outcome to DCS customer(s) and/or DIR as required.

(e) The Successful Respondent will cooperate with DIR in its attempts at transferring, replacing or augmenting the services responsibilities to another provider in a manner in keeping with not adversely affecting the provision of ongoing services and other projects being performed concurrent with this Service.

(f) Due to the nature of the Shared Technology Services program and the integration of SCPs therein, DIR expects that there may be occasions where an SCP's responsibilities may need to be revised to support the overall success of the program and ensure service continuity. DIR therefore retains the sole right to remove and/or reassign a portion of a SCP's scope as necessary. There may also be an occasion where DIR may ask that a SCP absorb work related to their scope of Services in an effort to provide continuity of service to the program where a gap may be discovered or a change for the betterment of the program may be needed. Should either of these actions be needed, the Successful Respondent will work with DIR in good faith to execute those changes through the appropriate Contract change request process. It is DIR's intent that the Successful Respondent will perform Services within the Shared Technology Services Program such that all actions support success of the program and prevent negative outcomes for Customers as may be anticipated and prevented by the Successful Respondent.

## 3.21. Successful Respondent Cooperation

(a) Successful Respondent shall perform the Services in a manner that shall not:

(i) disrupt or have an unnecessary adverse impact on the activities or operations of DIR, the DCS Customers, or a DIR Contractor;

(ii) degrade the Services then being received by DIR or the DCS Customers; or

(iii) disrupt or interfere with the ability of DIR or the DCS Customers to obtain the full benefit of the Services.

(b) Successful Respondent acknowledges that its provision of the Services shall require significant cooperation with third parties, and Successful Respondent shall fully cooperate and work in good faith with third parties as described in this Agreement and to the extent otherwise requested by DIR. DIR and DCS Customer personnel and DIR Contractors shall comply with Successful Respondent's reasonable security and confidentiality requirements and shall, to the extent performing work on Software, Equipment or Systems for which Successful Respondent has operational responsibility, comply with Successful Respondent's reasonable standards, methodologies, and procedures as communicated in writing to such third parties by Successful Respondent.

### 3.22. Onboarding New Customers

(a) The Successful Respondent will work with the MSI and other SCPs to support their new customer onboarding efforts in accordance with the established SMM and Operating Agreements.

(b) At Transition or as a new Customer or SCP joins the DCS Program, the Successful Respondent will:

(i) Perform a baseline assessment of the environment, according to the agreed assessment specifications as defined in the SMM, focusing on secure settings, logging, network services, and vulnerabilities;
(ii) Obtain DCS network tap and port aggregation flows from network devices for analysis through existing Data Capture & Analysis PODs (DCAP);
(iii) Incorporate each asset associated with the DCS backend infrastructure network devices, that are located within DCS service locations, that have been identified, and classified, in the previous stage as part of ongoing active scanning from the DCAP to determine open/listening network services (ports); and
(iv) Support the secure delivery of services from related SCPs.

(c) The Successful Respondent will perform tuning of data capture and analysis based on State-furnished information on normal and permissible traffic flows and identify and (to the extent possible) eliminate all non-permissible flows.

### 3.23. Performance Guarantee

The continuous operation of the Service and systems provided by the Security Operations Services SCP is vital to DCS Customers. For failures affecting critical components causing an interruption of service experienced by any in-scope system (outage), the Successful Respondent must agree to utilize any and all resources to immediately correct the cause of such outage at no additional expense to any impacted DCS Customer(s).

## 4. Steady State Evolution and Optimization of Services

### 4.1. Environment Review and Advisory Services

The Successful Respondent will support DIR, TSS and the MSI in the administration, implementation, optimization, and support of the use of the Service and service elements inclusive of all hardware, devices, tools, operational processes and emerging standards as to support DCS' position with respect to high performance, high quality, and high availability (to the extent contained and as applicable to the work in this Exhibit) Service infrastructure provided by the Successful Respondent in the performance of the contracted responsibilities under this Exhibit.

### 4.2. Technology Planning and Optimization Roadmap

(a) The Successful Respondent will participate with the TSS and MSI in the development of a multi-year Service roadmap inclusive of all projects, optimization and transformation initiatives. This review will be designed to ensure the ongoing support of steady state operations, future deployments and capabilities, extensions into new service delivery opportunities and customer growth. Additionally, this review will highlight strategic planning in support of State-wide and individual Customer

initiatives and identified use case opportunities to evolve services to better support the State's mission.

(b) The Technology Plan and Roadmap is an annual Critical Deliverable.

(c) The Successful Respondent will implement the optimization and technology improvements identified in the plan and approved by DIR.

(d) The Successful Respondent will:

(i) In coordination with the MSI, provide a process and ongoing program management for the establishment, currency, tracking, and publishing of a Technology Plan that incorporates input from DIR, DCS Customers, and SCPs and aligns with the governance processes.

(ii) Organize and participate in active cross-functional, cross-group, and cross-location meetings, information gathering, and communication work sessions related to technology planning and evolution.

(iii) Include iterations based on quarterly reviews with DIR and will include a rolling three (3) year projection of anticipated changes as provided by DIR (subject to DIR business and planning requirements.

(iv) As part of each annual planning cycle, provide specific, short-term steps and schedules for projects or changes expected to occur within the first twelve (12) months of each plan.

(v) Identify industry and technological trends that may impact DIR's and DCS Customers' plans including the identification and tracking of regulatory issues/changes that may impact DIR's plans.

(vi) Gather and incorporate the data and lessons learned from the operating environment that may impact DIR's and DCS Customers' plans and include trend analysis from the resource consumption data to project future demand that may impact DIR's and DCS Customers' plans.

### 4.2.1. Processes, Procedures, Architecture, Standards, and Planning

(a) As requested by DIR, Successful Respondent, without limiting the obligation of the Parties under **MSA, Section 8.11 Compliance with Laws**, shall assist DIR and the appropriate governance committee (as specified in Article 8 DCS Governance Model), on an on-going basis in defining:

(i) The standards, policies, practices, processes, procedures and controls to be adhered to and enforced by Successful Respondent in the performance of the Services, including those identified herein, and

(ii) The associated IT technologies architectures, standards, products and systems to be provided, operated, managed, supported and/or used by Successful Respondent in connection therewith (collectively, the "DIR Standards").

(b) The Parties acknowledge and agree that, as of the Commencement Date, Successful Respondent is fully informed as to the DIR Standards that have been communicated to it in a manner consistent with **MSA, Section 4.3 DIR Rules/Employee Safety**.

(c) Successful Respondent also shall assist DIR on an annual basis in preparing Technology Plans that include both long-term strategic and short-term implementation plans. The assistance to be provided by Successful Respondent shall include:

(i) Active participation with DIR and the appropriate governance committee (as specified in Article 8 DCS Governance Model), addressing such issues;
(ii) Assessments of the then-current DIR Standards at a level of detail sufficient to permit DIR to make informed business decisions;
(iii) Analyses of the appropriate direction for such DIR Standards;
(iv) The provision of information to DIR regarding Successful Respondent's technology strategies for its own business;
(v) Recommendations regarding standards, processes, procedures and controls and associated technology architectures, standards, products and systems; and
(vi) The provision of current, historical, and forecasted system capacity, performance and utilization metrics at reasonable requested levels of detail.

(d) With respect to each recommendation, Successful Respondent shall provide the following at a level of detail sufficient to permit DIR to make an informed business decision:

(i) The projected cost to DIR and the DCS Customers and cost/benefit analyses;
(ii) The changes, if any, in the personnel and other resources Successful Respondent, DIR and/or the DCS Customers shall require to operate and support the changed environment;
(iii) The resulting impact on the total costs of DIR and the DCS Customers;
(iv) The expected performance, quality, responsiveness, efficiency, reliability, security risks and other service levels; and
(v) general plans and projected time schedules for development and implementation. Any assistance provided by Successful Respondent under this section shall be at no additional fee or charge beyond the Charges specified in **Exhibit 2 Pricing** for the Services, unless an additional Charge has been approved by DIR.

(e) DIR shall have final authority to promulgate DIR Standards and Strategic Plans and to modify or grant waivers from such DIR Standards and Strategic Plans. Successful Respondent shall:

(i) Comply with and implement the DIR Standards and Strategic Plans in providing the Services;
(ii) Work with DIR to enforce the DIR Standards and Strategic Plans;
(iii) Modify the Services as and to the extent necessary and on a schedule to conform to such DIR Standards and Strategic Plans; and
(iv) Obtain DIR's prior written approval for any deviations from such DIR Standards and Strategic Plans.

### 4.2.2. Annual Security Review, Advisory and Planning Services

No less frequently than annually the Successful Respondent will provide advisory services and a report as an annual Deliverable as part of the MSI-led Annual Security Plan per **Attachment 1.1 Deliverables**. This effort is designed to assist the State in the administration, implementation, optimization and

support of the use of security services, devices, tools and emerging standards supporting DCS' position with respect to high performance, high quality and high availability DCS infrastructure provided by the Successful Respondent.

### 4.2.3. Annual Technology Planning Process

(a) The Successful Respondent shall adhere to the TSS and MSI process and ongoing program management for the establishment, currency, tracking, and publishing of a Technology Plan that incorporates input from DIR, TSS, MSI, DCS Customers, and SCPs and aligns with the governance processes.

(b) This plan will include but is not limited to:

(i) Introduction of new technologies, capabilities, and processes to drive more efficient and secure operations and DCS Customer experiences;
(ii) Implementation of new Service features and functions including wider deployment and use of DCS services, and extend the safe, secure, and available nature of DCS services to all DCS Customers and DCS Prospects;
(iii) Retirement of legacy Service elements and platforms where DCS provides similar or superior functional/technical footprints;
(iv) The automation of manual tasks associated with the Services including leading in the identification, solutioning and planning of MSI and/or Successful Respondent automation opportunities to increase automation, efficiencies, and value;
(v) Proactively identify strategies and approaches for future IT delivery that Successful Respondent believes will provide DIR and DCS Customers with competitive advantages and that may result in increased efficiency, performance, or cost savings; and
(vi) Evaluate market technology advances for Successful Respondent's tools and technologies that may provide DIR and DCS Customers greater capabilities, performance improvements, or improve Service Levels of the DCS environment. Tool selection will be in accordance with DIR and DCS Customers' standards and technical architectures.

### 4.2.4. Software Currency Requirements

#### 4.2.4.1. Currency of Software

Subject to and in accordance with **Attachment 2.1 Financial Responsibility Matrix**, Successful Respondent shall maintain reasonable currency for Software for which it is financially responsible under this Agreement and provide maintenance and support for Software (including new Upgrades, Major Releases, and Minor Releases) for which it is operationally responsible under this Agreement. At DIR's direction, Successful Respondent shall operate, maintain and support multiple releases or versions of the same Software without any increase in the Charges. In addition, unless otherwise directed by DIR, Successful Respondent shall keep Software within release levels supported by the appropriate third party vendor to maintain compatibility with other Software or Equipment components of the Systems and of DIR's Retained Systems and Processes. To the extent Third Party Software for which Successful Respondent is operationally responsible under this Agreement is no longer supported by the applicable licensor or manufacturer, Successful Respondent shall use commercially reasonable efforts to perform

maintenance for such Software as required. For purposes of this Section, "reasonable currency" means that, unless otherwise directed by DIR, Successful Respondent shall maintain Software within one (1) Major Release of the then-current Major Release, unless otherwise specified pursuant to the Software Currency guidelines set out in **Attachment 2.2 Financial Responsibility Matrix** and Successful Respondent shall install Minor Releases promptly or, if earlier, as requested by DIR.

#### 4.2.4.2. Evaluation and Testing

(a) Prior to installing a new Upgrade, Major Release, or Minor Release, Successful Respondent shall evaluate and test such Software to verify that it shall perform in accordance with this Agreement and the DIR Standards and that it shall not:

(i) increase DIR's or the DCS Customers' total cost of receiving the Services,
(ii) have an adverse impact on performance or require changes as described below; or
(iii) violate or be inconsistent with DIR Standards, DCS Technology Plans, or applicable Laws.

(b) The evaluation and testing performed by Successful Respondent shall be at least consistent with the reasonable and accepted industry norms applicable to the performance of such Services and shall be at least as rigorous and comprehensive as the evaluation and testing usually performed by highly qualified SCPs under such circumstances.

#### 4.2.4.3. Updates by DIR

DIR and the DCS Customers have the right, but not the obligation, to install new Upgrades, Major Releases or Minor Releases, replace or otherwise make any other changes to Software for which DIR is financially responsible under this Agreement.

#### 4.2.4.4. Approval by DIR or DCS Customer

(a) Successful Respondent shall seek approval from either DIR or the DCS Customer with control over the relevant software prior to installing any new Upgrade, Major Release or Minor Release. Successful Respondent shall provide DIR or DCS Customer with the results of its testing and evaluation of such Software and a detailed implementation plan and shall not install such Software if directed not to do so by DIR or DCS Customer. Where specified by DIR, Successful Respondent shall not install new Upgrades, Major Releases or Minor Releases or make other Software changes until DIR has completed and provided formal signoff on successful user acceptance testing. Successful Respondent shall not install new Upgrades, Major Releases or Minor Releases or make other Software changes if doing so would require DIR or the DCS Customers to install new releases of, replace or make any other changes to any Software for which DIR or DCS Customer is financially responsible under this Agreement unless DIR or DCS Customer consents to such change in advance.

(b) If DIR rejects Successful Respondent's proposed Upgrade or replacement of a Software version that is back-leveled such that it is no longer supported by the applicable Software manufacturer, Successful Respondent may be relieved from applicable Service Levels in accordance with **MSA, Section 5.2 Savings Clause.**

(c) Notwithstanding the other provisions of Section 4.2.3 Annual Technology Planning Process, if DIR rejects Successful Respondent's proposed Upgrade or replacement of a Software version that is back-leveled such that it is no longer supported by the applicable Software manufacturer and Successful Respondent is thereafter required to incur additional fees and expenses to obtain necessary maintenance for such Software version from such Software manufacturer in order to meet its obligations under this Agreement, DIR shall reimburse Successful Respondent for the reasonable fees and expenses thus incurred, but only if:

(i) Successful Respondent is unable, using commercially reasonable efforts, to perform such maintenance using Successful Respondent Personnel, including maintenance of knowledge among Successful Respondent Personnel about Software versions retained or desired to be retained by end users;
(ii) DIR has rejected Successful Respondent's proposed Upgrade or replacement of such Software version after being notified by Successful Respondent that it will not able to provide certain required maintenance for such Software version using Successful Respondent Personnel;
(iii) Successful Respondent notifies DIR of its intent to use such Software manufacturer to perform maintenance and the anticipated fees and expenses associated therewith and obtains DIR's approval prior to incurring such fees and expenses; and
(iv) Successful Respondent uses commercially reasonable efforts to minimize the fees and expenses to be reimbursed by DIR.

#### 4.2.4.5. Out of Support Third Party Equipment and Software

For Third Party Equipment and Third Party Materials consisting of Software that is no longer supported by the licensor or manufacturer for which Successful Respondent has operational responsibility under this Agreement, Successful Respondent shall use best efforts to perform maintenance for such Equipment or Software as required to meet its obligations under this Agreement.

### 4.2.5. Software Currency Management

Successful Respondent’s responsibilities include:

(i) Automated monitoring currency of hardware and software relative to respective vendor sources resident in each Successful Respondent’s technology plan and ensure proper notification is provided to DIR, DCS Customer, and Third-Party Vendors regarding support and software currency plans.
(ii) Unless otherwise directed by DIR, provide and support Software under Successful Respondent’s operational responsibility at the most recently released and generally available version of the Software (the “N” release level).
(iii) As directed by DIR, also support releases as specified in the Financial Responsibility Matrix.
(iv) Support Software that is no longer supported by the Third-Party Vendor.
(v) Provide support for all Software versions and release levels that exist as of the Effective Date until otherwise directed by DIR.

(vi) Provide monthly reports of upcoming software releases, software renewals and end-of-support notices on affected DCS Customers to the MSI, at least 180 days prior to expirations date.

### 4.2.6. Technology Adoption and Alignment

The Successful Respondent will provide information in the format required by the MSI to:

(i) Develop and structure the plan as to coordinate the aggregation of technical planning information from DIR, DCS Customers, Successful Respondent, and SCPs as directed by DIR and include an implementation roadmap, consistent with DIR's business roadmap with estimated timing, in alignment with the Technology Plan, for DIR and DCS Customers; and

(ii) Provide linkage with technology currency requirements that align with technology refresh plans (e.g., software version migrations) and include input from DIR to identify candidates and requirements for the deployment of new technology or the automation of tasks associated with the Services and/or DIR's and DCS Customers' business processes.

### 4.2.7. Technology Standards

The Successful Respondent will research and recommend standard products to the Technology Solution Services (TSS) for adoption into the program.

(i) Create and regularly (at least every ninety (90) days) update a description of minimum Equipment and Software requirements and specific Equipment and Software that are designated for standard use within DIR (the "Standard Products");

(ii) Publish and make available the description of Standard Products to Authorized Users as requested by DIR;

(iii) Make the description of Standard Products available on the MSI portal;

(iv) Align the Standard Product list with DIR's strategic direction, technical architecture, and refresh strategy;

(v) Provide mechanisms and processes to capture feedback and business needs from DCS Customers as to changes in Standard Products;

(vi) Maintain the Standard Products list on a relational database system, containing links/integration with the Asset Inventory and Management System as necessary and appropriate; and

(vii) Maintain all products in use as of Commencement and provide expertise for new standard products as they are added to the program.

### 4.2.8. Equipment Implementation and Refresh

Successful Respondent shall be fully responsible for the implementation of new Equipment in the ordinary course of Technology Evolution and Successful Respondent shall Refresh all Equipment in accordance with **MSA, Section 4.9 Change Control** and DIR's Refresh strategies, as set out in the Technology Plan, and as necessary to provide the Services in accordance with the Service Levels and satisfy its other obligations under this Agreement, which in all events shall be not less frequent than the Refresh guidelines set out in **Exhibit 2 Pricing**. If Successful Respondent is aware that these strategies

differ from generally accepted practice (or there are any other areas of concern in relation to such strategies) it shall provide DIR with notice of that fact and, upon request, provide DIR with further information as to how to more closely align the strategies with generally accepted practice.

## 4.3. Annual Review of Service Roadmap

(a) In conjunction with regularly scheduled operational meetings with DIR Personnel or a meeting of DCS Governance, and in driving continuous improvement requirements of this Exhibit, the Successful Respondent at least annually will sponsor a meeting to review recent or anticipated industry trends, emerging technologies, technology advancements, alternative processing approaches, new tools, methodologies or business processes (collectively "best practices") that, at DIR's choosing, could optimize the cost, efficiency, computing capacity, server density or otherwise drive efficiencies for both DCS Customers and the Successful Respondent.

(b) See **Attachment 1.1 Deliverables** for specific information regarding due dates, timelines, etc.

(c) Throughout the Term, Successful Respondent shall:

- (i) identify and apply best practice techniques, methods and technologies in the performance of the Services;
- (ii) train Successful Respondent Personnel in the use of new techniques, methods, and technologies that are in general use within Successful Respondent's organization and the IT and business consulting industries; and
- (iii) make necessary investments to keep and maintain the Software and other assets used to deliver the Services at the level of currency defined in this Section.

## 4.4. DIR Requested Projects

### 4.4.1. Procedures and Performance

Successful Respondent will perform Projects as directed by DIR, in accordance with the terms of this Agreement and the process defined by the MSI and described in the SMM. DIR may request Successful Respondent to perform Projects. DIR may initiate a request for a new Project by submitting a Request for Solution (RFS) via the MSI tool to Successful Respondent. Successful Respondent shall justify to DIR when it has insufficient resources to perform such work, including through reprioritization or rescheduling of Project activities of Successful Respondent Personnel. The DIR Representative will request, define and set the priority for Projects. Successful Respondent shall maintain appropriate continuity of personnel assigned to perform Projects.

### 4.4.2. Project Work Order

(a) Actively support the Demand Management process through development of technical solutions as initiated through Request for Solution procedures. This includes inter-tower solution development as well as supporting TSS in development of intra-tower solutions

(b) Successful Respondent shall, within the time frame and process specified in the SMM and at no charge to DIR, prepare and deliver to DIR a Solution Proposal Package (SPP), as described below. Each SPP prepared by Successful Respondent will contain the following information:

(i) a detailed description of the scope of work to be performed by Successful Respondent to complete and implement the Project, including any required Deliverables;

(ii) any specific performance standards that will apply to the completion and implementation of such Project, including Successful Respondent's agreement to meet applicable Service Levels;

(iii) an anticipated schedule for completing and implementing the Project and any related Deliverables, including Milestones and credits for failing to achieve Acceptance of Milestones and Deliverables;

(iv) a description of the Successful Respondent positions that will be assigned to each activity specified in the SPP, including the location of Successful Respondent Personnel assigned to such positions and sufficient detail to allow DIR to audit the assignment and billings related to such Successful Respondent Personnel;

(v) a description of the Acceptance Criteria and Acceptance Testing procedures to be used by DIR in connection with any Acceptance Testing of such Project and any related Deliverables and Milestones;

(vi) the estimated number of project personnel hours needed to complete the Project, as appropriate;

(vii) one (1) or more fee quotes, based on the following pricing mechanisms:

A. the applicable project bench rates,

B. if the Project consists of multiple units of work for which there are pre-defined one-time Charges, the number of pre-defined work units multiplied by the applicable pre-defined one-time Charge, or

C. if requested by DIR, a fixed fee or other pricing mechanism. DIR may, at its option, choose which pricing mechanism will apply to the Project.

(c) Successful Respondent will not commence performing any services in connection with a Project, and DIR will not be responsible for any Charges applicable to such Project, until the Parties have executed the applicable SPP. Any change to an approved Solution Proposal Package will be made pursuant to the Change Control Procedure.

### 4.4.3. Approval of Projects; DIR and DCS Customer Requests

The DIR Representative may accept or reject Solution proposals in his or her sole discretion. Successful Respondent shall not agree to implement any Solution Proposal to DIR or any DCS Customers without the prior approval of the designated Representative. DIR shall not be obligated to pay for any Projects not properly authorized by the designated DIR Representative. Without limiting DIR's other rights under this Agreement or applicable Law, if Successful Respondent fails to comply strictly with this Section, it shall receive no compensation for any services rendered to DIR or any DCS Customer in violation of this Section.

### 4.4.4. Reprioritization, Termination, and Suspension

Successful Respondent acknowledges and agrees that DIR will have the right based on valid business reasons to reprioritize, terminate, or suspend any Project at any time upon informing the Successful Respondent Contract Manager. DIR will not be obligated to pay Successful Respondent any additional compensation associated with such action unless the corresponding and approved or Solution Proposal Package expressly provides otherwise. If DIR decides to terminate a Project, Successful Respondent will

stop performing the Project work in an orderly manner as of the date specified by DIR, and Successful Respondent will only be entitled to charge DIR for actual performance provided by Successful Respondent for chargeable Project work up to the date specified in DIR's notice.

#### 4.4.5. Additional Work or Reprioritization

DIR may identify new or additional work activities to be performed by Successful Respondent's Personnel (including work activities that would otherwise be treated as New Services) or reprioritize or reset the schedule for existing Projects and other Services to be performed by Successful Respondent Personnel. Unless otherwise agreed, DIR shall incur no additional charges to the extent such work activities can be performed by Personnel then assigned to DIR. The Successful Respondent shall use commercially reasonable efforts to perform such work activities without impacting the established schedule for other tasks or the performance of the Services in accordance with the Service Levels. If it is not possible to avoid such an impact, Successful Respondent shall notify DIR in advance of the anticipated impact and obtain DIR's consent, in writing, prior to proceeding with such work activities. DIR, in its sole discretion, may forego or delay such work activities or temporarily adjust the work to be performed by Successful Respondent, the schedules associated therewith or the Service Levels to permit the performance by the Successful Respondent of such work activities.

## 5. Successful Respondent Personnel Requirements

**NOTE:** all roles (DIR minimum or otherwise) must be included in the Respondent Staffing Plan as required in this Section. For all DIR roles marked "as required," Respondents are to include (within their proposal) the staffing level required of DIR to ensure that the Successful Respondent project is staffed adequately.

### 5.1. Key Personnel Staffing

#### 5.1.1. Approval of Key Personnel

The positions designated by DIR to be filled by Key Personnel and the Key Personnel that have been selected and approved by DIR as of the Effective Date are identified in **Attachment 1.5 Key Personnel**. At least thirty (30) days prior to assigning an individual to act as one (1) of the Key Personnel, whether as an initial assignment or a subsequent assignment, Successful Respondent shall notify DIR of the proposed assignment, shall introduce the individual to appropriate DIR representatives, shall provide reasonable opportunity for DIR representatives to interview the individual and shall provide DIR with a resume and such other information about the individual as may be requested by DIR. If DIR in good faith objects to the proposed assignment, the Parties shall attempt to resolve DIR's concerns on a mutually agreeable basis. If the Parties have not been able to resolve DIR's concerns within five (5) DIR Business Days of DIR communicating its concerns, Successful Respondent shall not assign the individual to that position and shall propose to DIR the assignment of another individual of suitable ability and qualifications. DIR may add, delete, or otherwise change the positions to be filled by Key Personnel under this Agreement.

#### 5.1.2. Continuity of Key Personnel

(a) Successful Respondent shall cause each of the Key Personnel initially assigned at execution to devote full time effort to the provision of Services under this Agreement for, at a minimum, twenty-

four (24) months post Commencement. Successful Respondent shall cause each subsequent assignment of Key Personnel to devote full time effort to the provision of Services for, at a minimum, the applicable period specified by the Successful Respondent at the time of subsequent assignment, from the date he or she assumes the position in question (provided that, in the case of Key Personnel assigned prior to the Commencement Date, the minimum period shall be measured from the Commencement Date). Successful Respondent shall not transfer, reassign or remove any of the Key Personnel (except as a result of voluntary resignation, involuntary termination for cause, illness, disability, or death) or announce its intention to do so during the minimum period without DIR's prior approval, which DIR may withhold in its reasonable discretion based on its own self-interest. In the event of the voluntary resignation, involuntary termination for cause, illness, disability or death of one (1) of its Key Personnel during or after the specified period, Successful Respondent shall:

(i) give DIR as much notice as reasonably possible of such development, and
(ii) expeditiously identify and obtain DIR's approval of a suitable replacement.

(b) In addition, even after the initial twenty-four (24) month assignment period, Successful Respondent shall transfer, reassign, or remove one (1) of its Key Personnel only after:

(i) giving DIR at least thirty (30) days prior notice of such action (except to the extent such removal involves termination due to cause or performance as defined below);
(ii) identifying and obtaining DIR's approval of a suitable replacement at least thirty (30) days prior to such transfer, reassignment or removal;
(iii) providing DIR with a plan describing the steps and training (including knowledge transfer) that Successful Respondent shall perform to transition responsibility to the replacement; and
(iv) demonstrating to DIR's satisfaction that such action shall not have an adverse impact on Successful Respondent's performance of its obligations under this Agreement.

(c) Unless otherwise agreed, Successful Respondent shall not transfer, reassign, or remove more than one (1) of the Key Personnel in any six (6) month period; provided, however, the foregoing shall not prevent Successful Respondent from terminating a Key Personnel for cause or performance as defined below.

(d) For purposes of this Section cause means disregard of Successful Respondent's rules, insubordination, or misconduct (as defined in Successful Respondent's human resource policies), or criminal conduct, and performance means that the individual's job performance is at a level that would justify dismissal under Successful Respondent's human resources policies.

### 5.1.3. Retention and Succession

Successful Respondent shall implement and maintain a retention strategy designed to retain Key Personnel on DIR's and the DCS Customers' accounts for the prescribed period, such as retention bonuses. Successful Respondent shall also maintain active succession plans for each of the Key Personnel positions.

### 5.1.4. Successful Respondent Account Director

Successful Respondent shall designate an **Account Director** who, unless otherwise agreed by DIR, shall maintain his or her office in Austin, Texas. The Account Director shall:

(i) Represent (.5) of a Key Personnel resource;
(ii) be a full-time employee of the Successful Respondent;
(iii) devote 50% of his or her time and effort to managing the Services;
(iv) remain in this position for a minimum period of two (2) years from the initial assignment (except as a result of voluntary resignation, involuntary termination for cause, illness, disability, or death);
(v) serve as the single point of accountability for the Services;
(vi) be the single point of contact to whom all DIR communications concerning this Agreement may be addressed;
(vii) have authority to act on behalf of Successful Respondent in all day-to-day matters pertaining to this Agreement;
(viii) have day-to-day responsibility for service delivery, billing and relationship management; and
(ix) have day-to-day responsibility for ensuring customer satisfaction and attainment of all Service Levels.

## 5.2. Key Service Personnel Positions

(a) In an effort to foster a mutually supportive and collaborative environment in which the Services are provided in an effective manner that drives value to the State, the Parties will jointly review certain Key Successful Respondent Management and State Facing positions (collectively "Key Personnel"), including the Successful Respondent Account Representative. "Key Personnel" will include the following at a minimum:

(i) Account Director, as described in Section 5.1.4 Successful Respondent Account Director.
(ii) Technical Director with overall accountability for delivery of the Successful Respondent's requirements, technology planning, optimization, and innovation of Security Operations for this Service Component as well as other Service Components in Shared Technology Services.
(iii) Transition Director with overall accountability for delivery of the Successful Respondent's contract transition from contract execution through commencement of services, and through completion and DIR acceptance of all Transition deliverables.
(iv) Security Threat Intelligence Director with overall accountability for tracking and reporting on current and emerging threats and trends, working with the Technical Director and DIR to address current and planned for future threats to the STS environments.
(v) Other, as the Successful Respondent deems key to the fulfillment of its contract obligations.

(b) Key Personnel shall be committed for twenty-four (24) months minimum from contract execution unless stated otherwise. After twenty-four (24) months, replacement Key Personnel shall be committed for a minimum of twelve (12) months.

(c) Based on DIR's experience with DCS and similar managed services relationships with a variety of leading vendors, the State feels strongly the Successful Respondent team (as a team and as individuals) should be regularly reviewed with regard to several key factors including, but not limited to:

(i) Support of State DCS initiatives including DCS Customer and State Agency adoption of DCS and Infrastructure Consolidation;
(ii) Attainment of high customer satisfaction in Stakeholder (i.e., DCS Customers, DIR, Service Governance and DCS SCPs) communities and by extension and importantly end-user communities;
(iii) Creation of a highly integrated, collaborative and mutually supportive delivery of Services under this Exhibit to the State through the formation of an "integrated team" culture;
(iv) Adoption, implementation and refinement of a "State First" operating culture that is designed to drive value through the relationship and result in a high-performance working partnership between the State and Successful Respondent; and
(v) Incorporation of industry-leading and Successful Respondent best practices in the construction, operation, maintenance and support of DCS while seeking opportunities for continuous refinement and improvement of areas that are directly within the Successful Respondent's scope, those areas where the Successful Respondent has a reliance on the State and 3rd parties, and areas in the common interest of driving Service efficiency, quality and timeliness (e.g., value).

(d) The Successful Respondent, based on then current requirements, DIR preferences and strategies will assess its delivery team in light of DIR's direction and replace personnel as to align with the then current DIR standards, strategies and evolution roadmap of the in-scope Services within DCS. The Successful Respondent will ensure that the skills, experience, training and certification levels required to perform the Service, within the contracted service levels and volumes are contemporary with DCS Customer need and actively manage - through training, replacement, organizational design and components or other means - as to ensure that its personnel achieve DIR requirements.

(e) DIR and the Successful Respondent will meet on a regular basis, no less frequently than annually, to review the Successful Respondent's performance (as a team and as individuals) in driving toward these goals and agree to make changes to the number, nature, mix or named Key Personnel as required to improve and enhance the Successful Respondent's position in enabling DIR's attainment of these goals. As a one-time evaluation, the Successful Respondent and DIR shall review the performance of the entire Successful Respondent team within ninety (90) days of the Effective Date of this Contract as required herein and implement any changes such that the Service is launched with the best possible Successful Respondent team as possible.

(f) Should, for whatever reason, DIR determine based on documented or observed performance that a member (or members) of the Successful Respondent's Key Personnel is operating in a manner inconsistent with these goals, DIR will request a meeting of the Successful Respondent Account Representative and the DCS Administrator (and, if required, the State CIO, Successful Respondent Managing Director, Lead Partner for Public Sector or equivalent) to address localized or endemic failures to meet these goals. Upon receiving this feedback, the Successful Respondent will develop

and implement a plan to either realign the performance of the Key Personnel in question or replace them promptly should the situation dictate, in accordance with the provisions of this RFO pertaining to replacement personnel.

(g) For the avoidance of doubt, should for whatever reason the DCS Administrator request the replacement of any member of the Successful Respondent Staff, the Successful Respondent shall implement the change on a mutually agreeable schedule.

## 5.3. Staffing Requirements

### 5.3.1. Staffing Matrix/Model

(a) Successful Respondent shall provide a Staffing Plan including the following information:

(i) An organizational chart including any proposed subcontractors and key management and administrative personnel. All personnel identified as Key Personnel should be identified as part of the organizational chart. The organization chart must identify clear lines of authority and accountability within the organization;
(ii) A contingency plan that shows the ability to add more staff, if needed, to meet the Project's due date(s);
(iii) The number of people on site at the CDCs or other facilities at any given time;
(iv) A statement and a chart that clearly indicates the time commitment of the Respondent's Key Project Personnel to the DIR and state account;
(v) A statement indicating to what extent, if any, key personnel may work on other projects or assignments that are not related to the Services, during the term of the Contract. DIR may reject any proposal that commits the proposed Project Manager or any proposed Project Key Personnel to other projects during the term of the Project, if DIR believes that any such commitment may be detrimental to the Successful Respondent's performance.

(b) DIR reserves the right to identify certain roles proposed by the Successful Respondent as Key Personnel in addition to the Key Personnel that the Successful Respondent identifies.

### 5.3.2. Staffing Plan and Time Commitment

(a) The Successful Respondent shall provide a summary of full time equivalent (FTE) personnel needed for transition of the Services along with Service design and implementation in the Proposal document. Ongoing Staff Service Training

(a) The Successful Respondent will design and provide DIR with a formal Knowledge Transfer and Education Service in connection with any new service or new technology of the Successful Respondent's service. Successful Respondent shall:

(i) Educate and train its operational staff in the use its tools and processes; where appropriate. Successful Respondent shall provide this training to MSI and other SCP staff as required by DIR.
(ii) Create handover documentation, training, diagnostic scripts, and operational procedures for operations groups for all Services.

(iii) Provide operational training and documentation for support of Services to Respondent's staff, MSI staff, other SCP staff, DIR, and DCS Customers.

(iv) Conduct informal information sharing and knowledge transfer services concurrent with the implementation of any Service implementation or release. This knowledge transfer will ensure DCS Customer personnel assigned to support, develop, manage, or operate the Service platform are apprised of the contents of each release, features, functions, known defects and workarounds, and other information to manage and communicate to DIR and DCS Customer leadership (in general) and business stakeholders of the system and DCS Customer functional leaders (specifically) the most effective use of the then current system assets (i.e., the Service element(s), platform(s) and DCS Customer-developed enhancements or extensions).

(v) Develop materials such as Frequently Asked Questions (FAQs), one-pagers, how-to documents, or other help pages explaining the use of Services, as required. Materials shall comply with MSI publishing requirements as the MSI will publish these materials on its portal.

(vi) In an SMM, document the process workflow sufficient for the MSI and other SCP system staff to support the use of Successful Respondent's systems and Services to perform operational tasks, including, but not limited to the following tasks: simple configuration updates; moderate configuration updates; systems administration activities; and batch processing.

(b) Concurrently with any DCS Customer production implementation, the Successful Respondent will work with the MSI to develop knowledge articles that highlight specific system support processes, workflows, job aids, and updates arising from the solution implementation.

### 5.3.3. DCS Customer Training

The Successful Respondent will participate in MSI provided training as directed and support the MSI with training delivery for the Service (in general) and operational aspects of the service elements as to enable their use by DCS Customers. The MSI will determine the extent of Successful Respondent involvement in training delivery in addition to the minimum requirements below. As part of this activity area, the Successful Respondent will:

(i) Work with the MSI in the development, documentation, and delivery of workshops sufficient to prepare trainers and expert users for course delivery by focusing on the process and technical aspects of the training curriculum, including adult learning principles and facilitation techniques

(ii) Develop an approach and plan for DCS Customer support by:

A. Assisting the MSI in establishing a plan to manage the escalation of questions from training sessions and the communication of answers back out to trainers; and

B. Working with the MSI to develop an approach and plan for communicating with and training DIR stakeholders and vendors on the implemented modules and new business processes.

## 5.4. Replacement, Qualifications, and Retention of Successful Respondent Personnel

### 5.4.1. Sufficiency and Suitability of Personnel

(a) As a material obligation hereunder, Successful Respondent shall assign (or cause to be assigned) sufficient numbers of Successful Respondent Personnel to perform the Services in accordance with this Agreement (including applicable Service Levels), and such Successful Respondent Personnel shall possess suitable competence, ability and qualifications and shall be properly educated and trained for the Services they are to perform. Successful Respondent will maintain the organizational and administrative capacity and capabilities to carry out all Successful Respondent duties and responsibilities, including providing and supporting the Services, under this Agreement. Notwithstanding transfer or turnover of its personnel, or of its agents' or Subcontractors' personnel, Successful Respondent remains obligated to perform all duties and responsibilities, including providing and supporting the Services, without degradation and in accordance with the terms of this Agreement.

(b) Successful Respondent shall ensure staff have industry recognized security certifications aligned with NIST's National Initiative for Cybersecurity Education (NICE) – NICE Cybersecurity Workforce Framework (NCWF).

### 5.4.2. Responsibility for Successful Respondent Personnel

(a) Successful Respondent agrees that anyone used by Successful Respondent to fulfill the terms of this Agreement is an employee, agent or Subcontractor of Successful Respondent and remains under Successful Respondent's sole direction and control. In addition, Successful Respondent hereby agrees to be responsible for the following with respect to its employees, agents or Subcontractors:

(i) damages incurred by Successful Respondent Personnel or Subcontractors within the scope of their duties under this Agreement; and

(ii) determination of the hours to be worked and the duties to be performed by Successful Respondent Personnel or Subcontractors.

(b) Successful Respondent agrees and will inform its employees, agents, and Subcontractors that there is no right of action against DIR or any DCS Customer for any duty owed by Successful Respondent pursuant to this Agreement. Successful Respondent expressly agrees that neither DIR nor any DCS Customer assumes any liability for the actions of, or judgments rendered against, the Successful Respondent, its employees, agents, or Subcontractors. DIR's liability to the Successful Respondent's employees, agents, and Subcontractors, if any, will be governed by Chapter 101, Texas Civil Practice & Remedies Code.

### 5.4.3. Requested Replacement

In the event DIR determines that the continued assignment of any individual Successful Respondent Personnel (including Key Personnel) to the performance of the Services is not in the best interests of DIR, or any DCS Customer, then DIR may give Successful Respondent notice to that effect requesting that such Successful Respondent Personnel be replaced. Successful Respondent shall have ten (10) DIR Business Days following DIR's request for removal of such Successful Respondent Personnel in which to investigate the matters forming the basis of such request, correct any deficient performance, and

provide DIR with assurances that such deficient performance shall not recur (provided that, if requested to do so by DIR, Successful Respondent shall immediately remove (or cause to be removed) the individual in question from all DIR Facilities pending completion of Successful Respondent's investigation and discussions with DIR). If, following such ten (10) DIR Business Day period, DIR is not satisfied with the results of Successful Respondent's efforts to correct the deficient performance and/or to prevent its recurrence, Successful Respondent shall, as soon as possible, remove and replace such Successful Respondent Personnel with an individual of suitable and requisite ability and qualifications, at no additional cost to DIR. Nothing in this provision shall operate or be construed to limit Successful Respondent's responsibility for the acts or omissions of Successful Respondent Personnel or be construed as joint employment of the Successful Respondent Personnel.

### 5.4.4. Successful Respondent Personnel

(a) Successful Respondent shall be responsible for verifying:

- (i) that Successful Respondent Personnel are authorized to work in any location in which they are assigned to perform Services; and
- (ii) that it has performed pre-hire background investigations verifying that Successful Respondent Personnel had not been convicted of or accepted responsibility for a felony or a misdemeanor involving a dishonest act.

(b) Successful Respondent shall maintain policies prohibiting the use of illegal drugs. Successful Respondent represents that the Successful Respondent Personnel are not disqualified from performing their assigned work under applicable Laws.

### 5.4.5. CJIS Background and/or Criminal History Investigations

(a) The Successful Respondent is required to maintain CJIS compliance with staffing. Prior to the date any Successful Respondent Personnel are assigned to DIR's or any DCS Customer's account, and annually thereafter, background checks (including national fingerprint record checks and drug testing) and/or criminal history investigations of such Successful Respondent Personnel specified in the Service Management Manual or the applicable Statement of Work must be performed. Should any Successful Respondent Personnel not meet CJIS compliance as a result of a background check and/or criminal history investigation, then Successful Respondent shall promptly replace the individual(s) in question. Successful Respondent Personnel who do not meet CJIS compliance shall not be assigned to work hereunder.

(b) The Successful Respondent shall, at a minimum:

- (i) Limit access to and use of data to authorize Successful Respondent personnel only.
- (ii) Successful Respondent personnel must have received security clearance and successfully complete a background and criminal history investigation prior to performing contract functions or accessing DIR, DCS Customer Facilities, Systems, Networks or Data.
  - A. Criminal history background checks are to be conducted per Texas Government Code (TGC) Subchapter F, Section 411.1404 and will be in compliance with the then-current versions of the FBI CJIS Security Policy and the FBI CJIS Security Addendum. In addition, an annual background check re-verification is required.

Results of the initial background check and all annual reverifications must be documented in the MSI's Security Clearance and Tracking System.

B. Background and criminal history background checks will be performed by the Texas Department of Public Safety and the Texas Department of Criminal Justice. DCS Customers may require additional levels of compliance as per agency regulations and policies. Successful Respondent shall comply with any such additional levels of compliance including but not limited to CJIS.

C. Successful Respondent is responsible for any costs associated with the criminal history background check process.

D. Successful Respondent will establish a process that facilitates the timely submission and resolution of the criminal history background checks, including but not limited to using digital methods to submit necessary criminal history background check requirements.

(iii) Implement processes and procedures for tracking Clearances for all Successful Respondent personnel and Third-Party Vendors utilizing the Security Clearance Management System provided by the MSI.

## 5.5. Location of Services

(a) Services are to be performed at a combination of sites which must include the State of Texas computing locations. Permanent office space in the ADC and SDC is available for Successful Respondent Staff. There is no charge for the use of this space. Respondents must indicate in their Response whether it intends to make use of this space and for what number of staff. DIR prefers Successful Respondent staff to be located in ADC or SDC offices.

(b) **All services and data must remain within the continuous United States. Offshore access to any element of the Solution, Service, State specific deliverables, work products, technical details or other data is not permissible under any circumstances.**

## 5.6. Work Location(s) and Successful Respondent Personnel Involvement

See Successful Respondent Proposal Document.

## 5.7. Evergreen Service Personnel

(a) Based on DIR's experience with similar managed services relationships with a variety of leading vendors, DIR will regularly review that the Successful Respondent team (as a team and as individuals) regarding several key factors including, but not limited to:

(i) Enablement of DIR Service-related initiatives.

(ii) Attainment of high customer satisfaction in Stakeholder DCS Customer communities and by extension and importantly end-user communities.

(iii) Creation of a highly integrated, collaborative and mutually supportive delivery of Services under this Service to DCS Customers through the formation of an "integrated team" culture.

(iv) Adoption, implementation and refinement of a "State First" operating culture that is designed to drive value through the relationship and result in a high-performance working partnership between DIR and Successful Respondent.

(v) Incorporation of industry-leading and Successful Respondent best practices in the operation, maintenance and support of the Service while seeking opportunities for continuous refinement and improvement of areas that are directly within the Successful Respondent's scope, those areas where the Successful Respondent has a reliance on DIR, the MSI, DCS Customers and third parties, and areas in the common interest of driving Service efficiency, quality and timeliness (e.g., value).

(b) DIR and the Successful Respondent will meet on a regular basis, no less frequently than annually, to review the Successful Respondent's performance (as a team and as individuals) in driving toward these goals and agree to make changes to the number, nature, mix or named Key Personnel as required to improve and enhance the Successful Respondent's position in enabling DIR's attainment of these goals. As a one-time evaluation, the Successful Respondent and DIR shall review the performance of the entire Successful Respondent team within ninety (90) days of the Effective Date of this Agreement as required herein and implement any changes such that the Service is launched with the best possible Successful Respondent team as possible.

(c) Should, for whatever reason, DIR determine based on documented or observed performance that a member (or members) of the Successful Respondent's Key Personnel is operating in a manner inconsistent with these goals, DIR will request a meeting of the Successful Respondent Account Representative and the DCS Administrator (and, if required, the State CIO, Successful Respondent Managing Director, Lead Partner for Public Sector or equivalent) to address localized or endemic failures to meet these goals. Upon receiving this feedback, the Successful Respondent will develop and implement a plan to either realign the performance of the Key Personnel in question or replace them promptly should the situation dictate in accordance with the provisions of this RFO pertaining to replacement personnel.

(d) For the avoidance of doubt, should for whatever reason the DCS Administrator request the replacement of any member of the Successful Respondent Staff, the Successful Respondent shall implement the change on a mutually agreeable schedule.

(e) Should, for any reason described above DIR and Successful Respondent determine that a member of the Successful Respondent Key Personnel need replacement, this replacement shall occur no later than thirty (30) calendar days from DIR's request or as agreed.

## 5.8. Key Service Personnel

(a) In addition, the Respondent's proposal must identify all Key Service Personnel who will provide services as part of the resulting Contract. The Key Service Personnel are identified in Section 5.2 Key Service Personnel Positions. DIR expects the proposed named Key Service Personnel will be available as proposed. Resumes for the proposed candidates must be provided for all Key Service Personnel. Representative resumes are not acceptable. The resumes will be used to supplement the descriptive narrative provided by the Respondent regarding their proposed team.

(b) The resume (two (2) page limit per resume) of the proposed Key Service Personnel must include:

(i) Proposed Candidate's Name;
(ii) Proposed role on this Service;

(iii) Listings of competed projects (a minimum of two (2) references for each named Key Project Personnel) that are comparable to this Project or required similar skills based on the person's assigned role/responsibility on this Project. Each project listed should include: at a minimum, the beginning and ending dates, client/company name for which the work was performed, client contact information for sponsoring Directors, Managers or equivalent level position (name, phone number, email address, company name, etc.), project title, project description, and a detailed description of the person's role/responsibility on the project;

(iv) Education;

(v) Professional Licenses/Certifications/Memberships; and

(vi) Employment History.

(c) Based on DIR's experience with similar managed services relationships with a variety of leading vendors, DIR feels strongly that the Successful Respondent team (as a team and as individuals) should be regularly reviewed regarding several key factors including, but not limited to:

(i) Enablement of DIR Service-related initiatives;

(ii) Attainment of high customer satisfaction in Stakeholder DCS Customer communities and by extension and importantly end-user communities;

(iii) Creation of a highly integrated, collaborative and mutually supportive delivery of Services under this Service to DCS Customers through the formation of an "integrated team" culture;

(iv) Adoption, implementation and refinement of a "State First" operating culture that is designed to drive value through the relationship and result in a high-performance working partnership between DIR and Successful Respondent; and

(v) Incorporation of industry-leading and Successful Respondent best practices in the operation, maintenance and support of the Service while seeking opportunities for continuous refinement and improvement of areas that are directly within the Successful Respondent's scope, those areas where the Successful Respondent has a reliance on DIR, the MSI, DCS Customers and third parties, and areas in the common interest of driving Service efficiency, quality and timeliness (e.g., value).

(d) DIR and the Successful Respondent will meet on a regular basis, no less frequently than annually, to review the Successful Respondent's performance (as a team and as individuals) in driving toward these goals and agree to make changes to the number, nature, mix or named Key Personnel as required to improve and enhance the Successful Respondent's position in enabling DIR's attainment of these goals. As a one-time evaluation, the Successful Respondent and DIR shall review the performance of the entire Successful Respondent team within ninety (90) days of the Effective Date of this Contract as required herein and implement any changes such that the Service is launched with the best possible Successful Respondent team as possible.

(e) Should, for whatever reason, DIR determine based on documented or observed performance that a member (or members) of the Successful Respondent's Key Personnel is operating in a manner inconsistent with these goals, DIR will request a meeting of the Successful Respondent Account Representative and the DCS Administrator (and, if required, the State CIO, Successful Respondent Managing Director, Lead Partner for Public Sector or equivalent) to address localized or endemic failures to meet these goals. Upon receiving this feedback, the Successful Respondent will develop

and implement a plan to either realign the performance of the Key Personnel in question or replace them promptly should the situation dictate in accordance with the provisions of this RFO pertaining to replacement personnel.

(f) For the avoidance of doubt, should for whatever reason the DCS Administrator request the replacement of any member of the Successful Respondent Staff, the Successful Respondent shall implement the change on a mutually agreeable schedule.

(g) Should, for any reason described above DIR and Successful Respondent determine that a member of the Successful Respondent Key Personnel need replacement, this replacement shall occur no later than thirty (30) calendar days from DIR's request or as agreed.

### 5.9. Personnel Experience, Accreditation and Certification Requirements

(a) The Successful Respondent shall be responsible for securing and maintaining staff that meets the minimum education qualifications as described in the Exhibit and possess the stated experience and expertise required to complete the tasks outlined in this RFO.

(b) The Successful Respondent shall have experience with WAN and LAN protocols. The Respondent should also have individuals on the team with CISSP, CISM & CRISC, CEH, or similar credentials.

### 5.10. Transition Staffing Requirements

The Successful Respondent must ensure an effective and successful transition of Services that ensures the Successful Respondent operations staff are sufficiently trained and prepared to assume operations. Knowledge transfer must be performed such that steady-state operations personnel are prepared to perform Services with minimal to no disruption in performance.

## 6. Performance Model – Service Level Agreements

(a) As of the Commencement Date (or as otherwise specified), the Successful Respondent will meet or exceed all applicable Service Levels monthly, or as otherwise specified in the specific Service Level. Any Service Level Defaults prior to the Service Level Credit Start Date will not be considered in the evaluation of a Service Delivery Failure.

(b) Key Performance Indicators, Critical Service Levels, Key Service Levels, Operating Measures, One Time Critical Deliverables, and Recurring Critical Deliverables may be added or substituted by DIR during the Term. For example, such additions or substitutions may occur in conjunction with changes to the environment and the introduction of new Service, Equipment, Software, or means of Service delivery – provided, however, that where such change is a replacement or upgrade of existing technology, there shall be a presumption of equivalent or improved performance.

### 6.1. General

#### 6.1.1. General Performance Standards

In addition to the Service Levels contained herein and in **Attachment 1.2 Service Level Matrix**, beginning on the Commencement Date, Successful Respondent shall perform the Services at levels of accuracy, quality, completeness, timeliness, responsiveness, and resource efficiency that are at least equal to those received by DIR and the DCS Customers prior to such date. In addition, Successful Respondent

shall perform the Services at levels of accuracy, quality, completeness, timeliness, responsiveness, resource efficiency, and productivity that are at least equal to accepted industry standards of first tier providers of services that are the same as or similar to the Services. The foregoing provisions of this Subsection shall not be deemed to supersede the Service Levels.

### 6.1.2. Service Level Performance Standards

Beginning on the Commencement Date, Successful Respondent shall perform the Services so as to meet or exceed the Service Levels set forth in or otherwise in accordance with the Agreement.

### 6.1.3. Corrective Action Plan

(a) In the event that either (i) DIR reasonably determines that Successful Respondent has failed or is reasonably likely to fail to deliver the Services, or (ii) Successful Respondent has determined that it has failed or is reasonably likely to fail to deliver the Services, then DIR or Successful Respondent, as applicable, will notify the other Party of such failure (a "CAP Notice"). Concurrently with such CAP Notice, Successful Respondent will immediately take steps to mitigate any harmful effects of such failure, promptly (and in any event as soon as reasonably practical) perform a Root Cause Analysis, and prepare a corrective action plan (each a "Corrective Action Plan" or "CAP") with respect to such failure. If in DIR's judgment any such Correction Action Plan is not adequately addressing the failure, Successful Respondent will meet with DIR and its designees in accordance with Article 8 DCS Governance Model. Within thirty (30) calendar days of a CAP Notice, the Successful Respondent will provide DIR with a written plan (the " Corrective Action Plan") for improving the Successful Respondent's performance to address the failure identified in the CAP (CAP Failure Event), which shall include a specific implementation timetable and measurable success criteria. Within thirty (30) calendar days of plan submission, or such other timeframe agreed to by DIR, the Successful Respondent will implement the CAP, which will include making timely and appropriate investments in people, processes and technology. In addition, the Successful Respondent will demonstrate to DIR's reasonable satisfaction that the changes implemented by it have been made in normal operational processes to sustain compliant performance results in the future.

(b) Upon the occurrence of (1) if Successful Respondent has not submitted a Corrective Action Plan within the required thirty (30) days, (2) if the Corrective Action Plan has not, in DIR's judgment; remedied the CAP Failure Event, or (3) if the Successful Respondent fails to implement the Service Delivery Corrective Action Plan in the specified timetable or if after the implementation of the Service Delivery Corrective Action Plan performance has not consistently improved, then the Successful Respondent will be liable for a Service Level Credit in an amount equal to one percent (1 %) of the then-current Service Level Invoice Amount (the "CAP Failure Credit"). The CAP Failure Credit will be applied to the monthly invoice until the Successful Respondent has demonstrated effective Service delivery, as evidenced by either:

    (i) no reoccurrence of the Service Level Defaults which triggered the applicable Service Delivery Failure for a rolling three months; or
    (ii) in DIR's judgment, the Successful Respondent has remedied the failure which caused such Service Delivery Failure.

(c) The CAP Failure Credit will not be subject to Earnback (See Table 1: Terms and Definitions). The Successful Respondent acknowledges and agrees that the CAP Failure Credit shall not be deemed or construed to be liquidated damages or a sole and exclusive remedy or in derogation of any other rights and remedies DIR has hereunder or under the Agreement. For purposes of clarity, the CAP Failure Credit is separate from and therefore additive to any other Service Level Credits due in a given month, even if the Service Level Credits are for Service Level Defaults related to the Service Delivery Failure. In no event shall the sum of the CAP Failure Credit and any Service Level Credits credited to DIR with respect to all Service Level Defaults occurring in a single month exceed, in total, the At-Risk Amount.

#### 6.1.4. Additional Remedies

In the event that Successful Respondent fails to identify and resolve any problems that may impede or delay the timely delivery of the Services, without prejudice to DIR's other rights and remedies under the Agreement or at law or equity, Successful Respondent will immediately provide, at its sole cost and expense, all such additional resources as are necessary to identify and resolve any problems that may impede or delay the delivery of the Services. In addition, without prejudice to DIR's other rights and remedies under the Agreement or at law or equity, in the event of a CAP Failure Event, DIR may equitably reduce the Charges set forth in **Exhibit 2 Pricing** in an amount reasonably estimated by DIR to account for the Services that DIR and/or the DCS Customers are not receiving or did not receive.

### 6.2. Service Level Credits

Successful Respondent recognizes that DIR is paying Successful Respondent to deliver the Services at specified Service Levels. If Successful Respondent fails to meet such Service Levels, then, in addition to other remedies available to DIR, Successful Respondent shall pay or credit to DIR the Service Level Credits specified in **Attachment 1.2 Service Level Matrix** in recognition of the diminished value of the Services resulting from Successful Respondent's failure to meet the agreed upon level of performance, and not as a penalty. Under no circumstances shall the imposition of Service Level Credits be construed as DIR's sole or exclusive remedy for any failure to meet the Service Levels. Service Level Credits are not counted toward and are not subject to the overall cap on Successful Respondent's liability.

### 6.3. Shared and Related Service Levels and Types

(a) To clarify how specific Service Levels are intended to be tracked and calculated, individual Service Levels may be generally categorized as one (1) of two (2) types, representing the way individual SCPs and the Successful Respondent are either individually or jointly responsible for the specific Service Level's performance. Service Level Credits assessed against each SCP (or Successful Respondent) will be calculated based on the specific SCP's (or Successful Respondent's) Service Level Invoice Amount, At-Risk Amount, and Allocation of Pool Percentage.

(i) **Type R (related):** Type R Service Levels are related measures shared between the Successful Respondent and the SCP(s). Type R Service Levels for the Successful Respondent are measured in the aggregate, counting events for both the Successful Respondent and the SCP(s). For the SCP, the Type R Service Level measures a discrete subset of the same pool of events, the subset applicable to that SCP. The definition and descriptions of Type R Service Levels as well as the Service Level and Service Level remain identical in the related agreements for both the Successful Respondent, the

MSI and the applicable SCP(s) during the Term, unless otherwise documented as an exclusion in Service Level Definitions.

(ii) **Type U (unique):** Type U Service Levels are intended to measure Services that are specific to one (1) SCP's or the Successful Respondent's performance, and therefore are not shared.

(b) The groupings described above are intended to clarify Service Level types for tracking purposes; none of the Successful Respondent's obligations as fully described in the Agreement are limited by these groupings.

## 6.4. Reporting

(a) Unless otherwise specified, each Key Performance Indicator, Critical Service Level, Key Service Level, Operating Measure, Recurring Critical Deliverable, and One-Time Critical Deliverable shall be measured and reported by Customer and by DIR Shared Technology Service (DCS, MAS, Texas.gov, MSS, etc.) monthly. The Successful Respondent shall provide data to the MSI enabling the MSI to calculate and report Service Level performance. The Successful Respondent shall comply with the MSI's tools, processes, and reporting formats. The format, layout, and content of any reports shall be agreed between DIR and the Successful Respondent. The MSI will publish the Successful Respondent's monthly performance reports by the 20th calendar day of each month. Reporting on One-Time Critical Deliverables is only required until all One-Time Critical Deliverables are received and approved by DIR.

(b) The Successful Respondent will create and maintain detailed procedure documentation of its Service Level Agreement (SLA) measurement process used to collect SLA data and calculate SLA attainment. The process documentation must include quality assurance reviews and verification procedures. The measurement process must be automated to the extent possible, and any manual data collection steps must be clearly documented, verified and auditable. All methods, codes, and automated programs must be documented and provided to DIR for validation and approval. The Successful Respondent must ensure it tests and validates the accuracy and currency of the documentation and measurement process on a quarterly basis.

### 6.4.1. Data and Reports

Successful Respondent shall provide the MSI and DIR with:

(i) Data and reports pertaining to the performance of the Services and Successful Respondent's other obligations under this Agreement sufficient to permit the MSI and DIR to monitor and manage Successful Respondent's performance;

(ii) those reports described in **Appendix A Reports** and the SMM in the form and format and at the frequencies provided therein;

(iii) those reports required elsewhere under the terms of this Agreement;

(iv) those reports generated by DIR and the DCS Customers prior to the Commencement Date; and

(v) such additional reports as DIR may identify from time to time to be generated and delivered by Successful Respondent on an ad hoc or periodic basis (all such reports described in (i)-(v), the "**Reports**").

### 6.4.2. Back-Up Documentation

As part of the Services, Successful Respondent shall provide the MSI and DIR with such documentation and other information available to Successful Respondent (including original source documentation and data in its native format or in an alternative industry-standard format as requested by DIR) as may be requested by DIR from time to time in order to verify the accuracy of the Reports provided by Successful Respondent. In addition, Successful Respondent shall provide DIR with all documentation and other information requested by DIR from time to time to verify that Successful Respondent's performance of the Services is in compliance with the Service Levels and this Agreement.

### 6.4.3. Correction of Errors

Successful Respondent shall promptly correct any errors or inaccuracies in or with respect to the SLA performance data and reports as part of the Services and at no additional cost.

## 6.5. Service Level Default

(a) A Service Level Default occurs when performance for a particular Critical Service Level fails to meet the applicable Minimum Service Level. Service Level Credits shall not apply to Key Service Levels.

(b) **NOTE**: **Attachment 1.2 Service Level Matrix** describes the information required to calculate a Service Level Credit.

(c) In the event of a Service Level Default, the Successful Respondent shall provide DIR credits as defined below. For each Service Level Default, the Successful Respondent shall pay to DIR, a Service Level Credit that will be computed in accordance with the following formula:

(i) **Service Level Credit = A x B x C**

**Where:**

**A** = The Allocation of the Pool Percentage specified for the Performance Category in which the Service Level Default occurred as shown in **Attachment 1.2 Service Level Matrix**.

**B** = The Service Level Credit Allocation Percentage for which the Service Level Default occurred as shown in **Attachment 1.2 Service Level Matrix**.

**C** = The At-Risk Amount

(d) For example, assume that the Successful Respondent fails to meet the Service Level for a Critical Service Level, the Successful Respondent's Service Level Invoice Amount for the month in which the Service Level Default occurred was $100,000 and that the At-Risk Amount is fifteen percent (15%) of these charges. Additionally, assume that Allocation of Pool Percentage for the Performance Category of such Critical Service Level is fifty percent (50%) and that its Service Level Credit Allocation Percentage is forty percent (40%). The Service Level Credit due to DIR for such Service Level Default would be computed as follows:

A = 50% (the Allocation of Pool Percentage) multiplied by

B = 40% (the Service Level Credit Allocation Percentage) multiplied by

C = $15,000 (fifteen percent (15%) of $100,000, the Successful Respondent's corresponding Service Level Invoice Amount)

= $3,000 (the amount of the Service Level Credit)

(e) If more than one (1) Service Level Default has occurred in a single month, the sum of the corresponding Service Level Credits shall be credited to DIR.

(f) In no event shall the amount of Service Level Credits credited to DIR with respect to all Service Level Defaults occurring in a single month exceed, in total, the At-Risk Amount.

(g) The total amount of obligated Service Level Credits shall be credited on the following month (i.e., defaults occurring in August shall be included in the September invoice).

(h) The Successful Respondent acknowledges and agrees that the Service Level Credits shall not be deemed or construed to be liquidated damages or a sole and exclusive remedy or in derogation of any other rights and remedies DIR has hereunder or under the Agreement.

## 6.6. Earnback

The Successful Respondent shall have Earnback opportunities with respect to Service Level Credits as follows:

(i) The Successful Respondent shall earn back fifty percent (50%) of a Service Level Credit for a given Service Level Default when Service Level Performance for the Service Level that experienced a default meets or exceeds the Service Level Target for each of the three (3) Measurement Windows immediately following the Measurement Window in which the Service Level Default occurred. The remaining fifty percent (50%) may be earned back when Service Level Performance meets or exceeds the Service Level Target for each of the three (3) Measurement Windows following the initial Earnback.

(ii) Whenever the Successful Respondent is entitled to an Earnback, the Successful Respondent shall include such Earnback as a charge to DIR (indicated as an Earnback) on the same invoice that contains charges for the Measurement Window giving rise to such Earnback and include such information in the Successful Respondent's monthly performance reports.

(iii) Upon termination or expiration of the Agreement, Service Level Credits issued by the Successful Respondent are no longer subject to Earnback.

## 6.7. Additions, Modifications, and Deletions of Service Levels

(a) By written notice, DIR may add, modify or delete Key Performance Indicators, Critical Service Levels, Key Service Levels, and Operating Measures as described below.

(b) DIR will provide at least ninety (90) calendar days' notice that additions or deletions to Performance Measures, (which include the movement of Critical Service Levels to Key Service Levels, and Key Service Levels to Critical Service Levels), or modifications to Service Level Credit Allocation Percentages for any Critical Service Levels, modifications to Critical Service Levels and Key Service Levels measurement methodologies, or additions or deletions to Recurring Critical Deliverables are to be effective. DIR may send only one (1) such notice (which notice may contain multiple changes) each calendar quarter. Movement of Critical Service Levels to Key Service Levels and Key Service Levels to Critical Service Levels does not constitute creation of new Service Levels.

### 6.7.1. Additions

DIR may add Service Levels in accordance with Section 6.7 Additions, Modifications, and Deletions of Service Levels. Service Level commitments associated with added Service Levels will be determined as follows:

(i) The Parties shall attempt in good faith to agree on a Service Level commitment using industry standard measures or third-party advisory services (e.g., Gartner Group, Forrester, etc.).

(ii) With respect to this individual Service Level, the period between the Statement of Work (SOW) Commencement Date and the Service Level Effective Date shall be used as a validation period. The Successful Respondent and DIR will review the actual Service Level Performance during this validation period. If the Service Level Performance does not generally meet the Service Level Minimum, the Successful Respondent will create a corrective action plan subject to DIR's approval, and the Parties will extend the validation period (reset the Service Level Effective Date) by a mutually agreed period not to exceed three (3) months. The Successful Respondent will implement the corrective action plan and report on progress to DIR during the extended validation period. This process may be repeated if mutually agreed by the Parties. If the Parties eventually agree that the Services must be changed (e.g., staffing or Restoration time targets) or the Service Level Minimum must be revised, the Parties will enact such agreed changes through the Change Control Procedures.

### 6.7.2. Modifications

(a) DIR may modify Service Level commitments or measurement methodology in accordance with Section 6.7 Additions, Modifications, and Deletions of Service Levels. The Successful Respondent may propose modifications to Service Level measurement methodology for DIR approval. Service Level measurement methodology may be modified by updating **Attachment 1.3 Service Level Definitions**.

(b) For any Service Level commitments associated with modified service levels, the Parties shall attempt in good faith to agree on any modifications to current Service Level commitments using industry standard measures or third-party advisory services. In the event the Parties cannot agree on proposed modifications, **MSA, Section 12 Dispute Resolution** applies.

### 6.7.3. Deletions

DIR may delete Critical Service Levels or Key Service Levels by sending written notice in accordance with Section 6.7 Additions, Modifications, and Deletions of Service Levels.

### 6.7.4. Impact of Additions and Deletions of Critical Service Levels on Service Level Credit Allocation Percentages

(a) When adding or deleting a Critical Service Level, DIR shall modify the Service Level Credit Allocation Percentages for the Critical Service Levels such that the total Service Level Credit Allocation Percentages for all Critical Service Levels sums to less than or equal to Pool Percentage Available for Allocation.

(b) If DIR adds a Critical Service Level but does not modify the Service Level Credit Allocation Percentages for the Critical Service Levels then, until DIR so modifies such Service Level Credit Allocation Percentages, the Service Level Credit Allocation Percentage for such added Critical Service Level shall be zero (0).

### 6.7.5. Modifications of Service Level Credit Allocation Percentages for Critical Service Levels

DIR may modify the Service Level Credit Allocation Percentages for any Critical Service Levels by sending written notice in accordance with Section 6.7 Additions, Modifications, and Deletions of Service Levels. DIR shall modify the Service Level Credit Allocation Percentages for two (2) or more of the Critical Service Levels such that the sum of the Service Level Credit Allocation Percentages for all Critical Service Levels is less than or equal to the Pool Percentage Available for Allocation.

## 6.8. Service Delivery Failure: Corrective Action Plan

(a) If three (3) Service Level Defaults for the same Critical Service Level occur in any six (6) month period, then upon such third occurrence, this shall be deemed a "Service Delivery Failure." Within thirty (30) calendar days of a Service Delivery Failure, the Successful Respondent will provide DIR with a written plan (the "Service Delivery Corrective Action Plan (CAP)") for improving the Successful Respondent's performance to address the Service Delivery Failure, which shall include a specific implementation timetable and measurable success criteria. Within thirty (30) calendar days of plan submission, or such other timeframe agreed to by DIR, the Successful Respondent will implement the Service Delivery Corrective Action Plan (CAP), which will include making timely and appropriate investments in people, processes and technology. In addition, the Successful Respondent will demonstrate to DIR's reasonable satisfaction that the changes implemented by it have been made in normal operational processes to sustain compliant performance results in the future.

(b) The Successful Respondent will be liable for a Service Level Credit in an amount equal to one percent (1 %) of the then-current Service Level Invoice Amount (the "CAP Failure Credit") upon the occurrence of:

    (i) a Service Delivery Failure, or
    (ii) if the Successful Respondent fails to implement the Service Delivery Corrective Action Plan in the specified timetable, or
    (iii) if after the implementation of the Service Delivery Corrective Action Plan performance has not consistently improved.

(c) The CAP Failure Credit will be applied to the monthly invoice until the Successful Respondent has demonstrated effective Service delivery, as evidenced by either:

    (i) no reoccurrence of the Service Level Defaults which triggered the applicable Service Delivery Failure for a rolling three (3) months, or
    (ii) in DIR's judgment, the Successful Respondent has remedied the failure which caused such Service Delivery Failure.

(d) The CAP Failure Credit will not be subject to Earnback. The Successful Respondent acknowledges and agrees that the CAP Failure Credit shall not be deemed or construed to be liquidated damages or a sole and exclusive remedy or in derogation of any other rights and remedies DIR has hereunder

or under the Agreement. For purposes of clarity, the CAP Failure Credit is separate from and therefore additive to any other Service Level Credits due in a given month, even if the Service Level Credits are for Service Level Defaults related to the Service Delivery Failure. In no event shall the sum of the CAP Failure Credit and any Service Level Credits credited to DIR with respect to all Service Level Defaults occurring in a single month exceed, in total, the At-Risk Amount.

## 6.9. Service Level Improvement Plans

(a) If the Successful Respondent fails to meet any Minimum Service Level for a Critical Service Level for any one (1) or more DCS Customer or for the enterprise as a whole, the Successful Respondent shall follow the MSI's performance management process to provide DIR with a written Service Level Improvement Plan (SLIP) for improving the Successful Respondent's performance to satisfy the Service Level within thirty calendar (30) days of the failure to meet the Service Level. The objective of a Service Level Improvement Plan is to identify the root cause and formulate corrective actions to move performance to acceptable levels, implement those actions, and to correlate implemented corrective actions with Service Level results. All SLIPs must contain information about the root cause of the Service Level miss and corrective actions. All approved SLIP corrective actions shall be measured in the Corrective Action SLA results. The Successful Respondent will track its progress in implementing the improvement plan and it will report to Governance the status of such plan. The MSI will initiate a SLIP via the standard Problem Management Process when a Service Level underperforms. The Successful Respondent shall comply with the SLIP.

(b) DIR may also require overall SLIPs for Successful Respondent performance not directly related to an SLA that is impacting service delivery.

(c) Customer SLIPs are not required when the Critical Service Level for the performance period has a low volume of instances where the results missed the minimum. A Customer SLIP will be initiated when the difference between the numerator and the denominator is > Minimum Miss Threshold, or, SLA breach occurrences are > Minimum Miss Frequency within the Minimum Miss Frequency Timeframe. The Minimum Miss Threshold, Minimum Miss Frequency, and Minimum Miss Frequency Timeframe values are defined in the SMM for each Critical Service Level.

## 6.10. Service Level Escalation Event

(a) A Service Level Escalation Event occurs, if:

(i) the Successful Respondent asserts that it has been unable to perform all or a portion of the Services measured by a Type R Service Level solely as a result of the failure by another SCP or the MSI with whom it shares such Type R Service Level to perform obligations specified in the Successful Respondent's agreement with DIR, including its SOWs and the SMM, and

(ii) the Successful Respondent has performed its own obligations as set forth in the Agreement, including the SOWs and SMM, which actions shall include:

A. immediately notifying DIR, SCP(s) and MSI that such failure may result in a Service Level Default;

B. providing the SCP or MSI with reasonable opportunity to correct such failure to perform and thereby avoid the SCP or MSI non-performance;

C. documenting that it has performed its obligations under the Agreement notwithstanding another SCP's or MSI's failure to perform; and
D. notifying DIR that a corrective action has commenced.

(b) Upon the occurrence of a Service Level Escalation Event, the Successful Respondent may escalate the SCP or MSI failure through the appropriate governance structure for resolution in accordance with Section 8 DCS Governance Model.

(c) If the applicable governance committee has determined that the Successful Respondent has satisfied each of the requirements and obligations set forth above, such resolution shall include excusing the Successful Respondent's performance related to such failure and may include other actions as reasonably determined by DIR including appropriate changes to the SMM.

## 6.11. Service Level Definitions

Refer to **Attachment 1.2 Service Level Matrix** and **Attachment 1.3 Service Level Definitions and Performance Analytics** for detailed SLA definitions and measurement methodologies.

## 6.12. Recurring Critical Deliverables

(a) Certain of the Successful Respondent's obligations under the Agreement are periodic obligations to deliver key Recurring Critical Deliverables. Refer to **Attachment 1.1 Deliverables** and **Attachment 1.2 Service Levels Matrix** for amounts payable and frequency. Imposition of a Recurring Critical Deliverables Credit for failure to meet the Recurring Critical Deliverables obligations shall not be subject to or included in the At-Risk Amount. The total amount of Recurring Critical Deliverables Credit that the Successful Respondent will be obligated to pay to DIR shall be reflected on the invoice that contains charges for the month following which the Recurring Critical Deliverables Credits accrued (for example, the amount of Recurring Critical Deliverables Credits payable for failure to deliver any Recurring Critical Deliverable(s) in August shall be set forth in the invoice for September charges issued in October). Under no circumstances shall the imposition of the Recurring Critical Deliverables Credit described above, or DIR's assertion of any other rights hereunder be construed as DIR's sole or exclusive remedy for any failures described hereunder.

(b) DIR may add, modify, or delete Recurring Critical Deliverables by sending written notice, provided that after the implementation of any such addition or modification the aggregate amount of the Recurring Critical Deliverables Credits will not exceed the maximum amount of Recurring Critical Deliverables Credits set forth in **Attachment 1.2 Service Level Matrix**.

## 6.13. One-Time Critical Deliverables – After Effective Date

Certain of the Successful Respondent's obligations under the Agreement are one-time or periodic obligations to deliver One-Time Critical Deliverables. Refer to **Attachment 1.1 Deliverables** and **Attachment 1.2 Service Levels Matrix** for amounts payable and frequency. Imposition of Deliverable Credits for failure to meet the One-Time Critical Deliverables obligations shall not be subject to or included in the At-Risk Amount. The total amount of Deliverable Credits that the Successful Respondent will be obligated to pay to DIR shall be reflected on the invoice that contains charges for the month following which the Deliverable Credits accrued (for example, the amount of Deliverable Credits payable

for failure to deliver any One-Time Critical Deliverable(s) in August shall be set forth in the invoice for September charges).

## 6.14. Data Collection and Measuring Tools

(a) The Successful Respondent shall propose, and upon DIR's written approval, implement a data collection methodology for all Service Levels prior to the date upon which the Successful Respondent shall be responsible for Service Level performance. Failure to do so may be deemed a Service Level Default for the Service Level until the Successful Respondent proposes and implements such acceptable data collection. All data collection tools must be integrated with the MSI's performance management and reporting tool.

(b) Tools for new Service Levels will be implemented according to the Change Control Procedures. Upon DIR's written notice approving a proposed alternate or new measurement tool, such tool shall be deemed automatically incorporated into **Attachment 1.3 Service Level Definitions and Performance Analytics** as of the date for completion of implementation set forth in DIR's notification without requirement for an additional written amendment of this Agreement.

(c) If, after the Effective Date or the implementation of tools for new Service Levels, the Successful Respondent desires to use a different data collection tool for a Service Level, the Successful Respondent shall provide written notice to DIR, in which event the Parties will reasonably adjust the measurements as necessary to account for any increased or decreased sensitivity in the new measuring tools; provided that, if the Parties cannot agree on the required adjustment, the Successful Respondent will continue to use the data collection tool that had been initially approved by DIR.

(d) It is not anticipated that changes in the data collection tools will drive changes in Service Levels; rather, the need to collect and accurately reflect the performance data should drive the development or change in performance monitoring tools. The Successful Respondent will configure all data collection tools to create an auditable record of each user access to the tool and any actions taken with respect to the data measured by or residing within the tool. All proposed measuring tools must include functionality enabling such creation of an auditable record for all accesses to the tool.

## 6.15. Percentage Objectives

Certain Service Levels may not be measured against an objective of one hundred percent (100%); for example, time (days, hours, etc.), defects where zero (0) hours/days and zero percent (0%), respectively, are the appropriate objectives. The calculations described in this Section will be modified when appropriate to reflect these objectives.

## 6.16. Low Volume

(a) Some Service Levels are expressed in terms of achievement of a level of performance over a percentage of items occurring during a Measurement Window. In these instances, if the number of items occurring during a given Measurement Window is less than or equal to one hundred (100), the following algorithm will be used to determine the number of compliant items that Successful Respondent must successfully complete to achieve the Service Level concerned (Minimum

Compliant Items), notwithstanding the percentage expressed in **Attachment 1.2 Service Level Matrix** as the target.

(i) The number of items occurring during such Measurement Window shall be multiplied by the Service Level Target; and

(ii) If the product of that multiplication is not a whole number, then such product shall be truncated to a whole number.

(b) For example, assume that a Service Level states that the Successful Respondent must complete ninety-five percent (95%) of incidents within four (4) hours to achieve this Service Level.

(i) The following sample calculations illustrate how the above algorithm would function to determine the Minimum Compliant Items (incidents completed within four (4) hours) to achieve this Service Level, in each case given a different number of total incidents occurring during the corresponding Measurement Window:

(ii) If the number of incidents is 100, the Minimum Compliant Items is 95 incidents (100 incidents x 95 percent = 95 incidents).

(iii) If the number of incidents is 99, the Minimum Compliant Items is 94 incidents (99 incidents x 95 percent = 94.05 incidents, truncated to 94).

(iv) If the number of incidents is nine (9), the Minimum Compliant Items is eight (8) incidents (9 incidents x 95 percent = 8.55 incidents, truncated to 8).

**Table 6: SLA Translation**

| Target | Service Level |
|---|---|
| Number of Items | Minimum Compliant Items |
| 100 | 95 |
| 90 | 85 |
| 80 | 76 |
| 70 | 66 |
| 60 | 57 |
| 50 | 45 |
| 40 | 38 |
| 30 | 28 |
| 20 | 19 |
| 10 | 9 |

## 6.17. Service Levels Review

(a) **Initial Review:** Within six (6) months of the Service Commencement Date or completion of Transition as outlined in this Exhibit, whichever is sooner, or as agreed to by both parties, the Parties will meet to review the initial Service Levels and Successful Respondent's performance and discuss possible modifications to the Service Levels. Any changes to the Service Levels will be only as agreed upon in writing by the Parties.

(b) **Annual Review:** Every year following the Service Commencement Date or completion of Transition as outlined in this Exhibit, the Parties will meet to review the Service Levels and Successful Respondent's performance in the period of time since the prior review and discuss possible

modifications to the Service Levels. Any changes to the Service Levels will be managed according to the requirements in Section 6.7 Additions, Modifications, and Deletions of Service Levels.

### 6.17.1. Temporary Escalation of a Key Service Level to a Critical Service Level

(a) In general, Key Service Levels are considered measurable objectives by DIR and the SLA framework accommodates their treatment and importance to DIR. In the event that Successful Respondent performance is not meeting the established standards and requirements for Key Service Level related items, DIR may determine that a Key Service Level needs to be escalated to a Critical SLA. The following conditions shall prevail in this escalation:

(i) Successful Respondent performance falls below the Minimum Service Level for a Key Service Level for three (3) consecutive months; or

(ii) Successful Respondent performance is consistently below the Minimum Service Level for four (4) of any six (6) consecutive months.

(b) Should one (1) or more of these conditions exist, DIR may:

(i) Temporarily replace any Critical Service Level of its choosing with the Key Service Level until such time as the below standard SLA is determined to be consistently (i.e., more than three (3) months in a row) performing to standard;

(ii) Promote the Key Service Level to the Critical Service Level modify the Service Level Allocation Percentages for the Critical Service Levels such that the total Service Level Credit Allocation Percentages for all Critical Service Levels sums to less than or equal to Pool Percentage Available, until such time as the below standard SLA is determined to be consistently (i.e., more than three (3) months in a row) performing to standard.

(c) At the conclusion of three (3) consecutive months where the escalated Key SLA is deemed to be performing at or above the Minimum Service Level, DIR may revert the escalated Key Service Level (now a Critical Service Level) back to its Key Service Level state.

## 6.18. Key Performance Indicators

(a) DIR requires Key Performance Indicators (KPIs) calculated on a dynamic, near real-time basis, utilizing the most current data. There will also be a need to report the KPIs on a monthly basis for governance purposes; however, the intent is to provide DIR with continuous updates throughout the month to facilitate strategy around future business direction. Weightings for the Operating Measurements (OM) will be maintained in the SMM.

(b) The qualitative descriptions of the KPIs are set forth in **Attachment 1.3 Service Level Definitions and Performance Analytics**. The strategic objectives and commencement of obligations associated with such Key Performance Indicators are set forth in **Attachment 1.2 Service Level Matrix**. KPIs are not Service Levels and are not subject to Service Level Credits.

(c) DIR's use of KPI's is for the sole purpose of accurately measuring the health of the Shared Services Program and while DIR retains the right to adjust numeric ratings at its sole discretion, DIR will collaborate with the Successful Respondent and SCPs to identify appropriate numeric ratings for the KPIs.

## 6.19. Operating Measurements

(a) The qualitative descriptions of the OMs are set forth in **Attachment 1.3 Service Level Definitions and Performance Analytics**. These are linked to the KPIs as described in Section 6.18 Key Performance Indicators and **Attachment 1.3 Service Level Definitions and Performance Analytics**. The business objectives and commencement of obligations associated with such Operating Measurements are set forth in **Attachment 1.2 Service Level Matrix**.

(b) To ensure visibility of progress toward business and strategic objectives, the Successful Respondent will report Operating Measurements.

(c) To ensure the integrated and seamless delivery of the Services, the Successful Respondent is required to report Operating Measurements that measure the dependencies with each SCP.

## 6.20. Operational Reports

The Successful Respondent's responsibilities include, at a minimum:

(i) Providing all Reports currently being provided by the Incumbent Service Provider, including:
   A. Those Reports listed in **Appendix A Reports**, including those reports contemplated in **Appendix A Reports**, but not in production;
   B. According to the format, content, and frequency as noted in **Appendix A Reports**;
   C. In compliance with report specifications identified in a formal report development process (e.g., requirements, development, test, acceptance, production ready) to be completed for each designated Report prior to the Commencement Date.

(ii) Providing ad hoc reports as requested by DIR in compliance with processes outlined in the Service Management Manual.
   A. Where practical provide the capability for DIR and DCS Customers to request Reports based on standard data provided via the Portal.
   B. Provide capability for DIR or DCS Customer to generate ad hoc reports via the reporting tool.

(iii) Delivering all Reports requested within other documents that are referenced as requirements in other Exhibits.

(iv) Modifying the format, content, and frequency of any Report as requested by DIR during the Term, subject to Change Management procedures.

(v) At a minimum, provide all Reports via the Portal through a real-time web-accessible reporting dashboard.

(vi) Provide access statistics for Reports presented via the Portal at the request of DIR.

(vii) Providing soft or hard copies of Reports as requested by DIR.

## 6.21. Single Incident/Multiple Defaults

If a single incident results in the failure of the Successful Respondent to meet more than one (1) Service Level, DIR shall have the right to select any one (1) of such multiple Service Level Defaults for which it

will be entitled to receive a Service Level Credit and will respond to the Successful Respondent's reporting of the multiple Service Level Default and request for selection by notifying the Successful Respondent of the selection within five (5) DIR Business Days. DIR shall not be entitled to a Service Level Credit for each of such Service Level Defaults.

### 6.22. Exceptions

The Successful Respondent shall not be responsible for a failure to meet any Service Level solely to the extent that such failure is directly attributable to any circumstances that excuse the Successful Respondent's performance in accordance with **MSA, Section 5.2 Savings Clause**.

### 6.23. Exclusions

Any incidents or requests opened prior to Commencement Date by DIR are excluded from SLA measurements and will be tracked separately. Additional exclusions are indicated in **Attachment 1.3 Service Level Definitions and Performance Analytics.**

## 7. Transformation Projects

### 7.1. Organization and Relationship of Transformation Projects

(a) Transformational projects are optional; The numbering of these projects is **purely for identifying purposes only**. DIR may instruct the Successful Respondent to complete these transformation projects, in whole or part, in any order and at any time during the Contract or may elect not to undertake any of the transformational projects listed herein.

(b) DCS platforms are in constant stages of development, maturity and adoption. A general overview of the current state of the security systems with their anticipated roadmaps is as follows:

**Table 7: Security Systems Current State and Anticipated Road Map**

| Project | Multi-Cloud Security Integration | Hardened Security and Standardization |
|---|---|---|
| General Strategy | Include public cloud assets as "trusted peers" within a Texas DCS cloud in every way and drive security, parity, agility and consistency across all private/public cloud assets | Move to a "templated" security and management model to ensure consistency, drive repeatability and ensure protection of State data and systems at all times |
| Status | Public cloud asset usage differs from on-premise security workflows, standards, tools and processes | DCS Customers are subject to multiple security, privacy and data handling requirements via State and Federal standards |

(c) As part of evaluation, DIR will review Respondent-proposed approaches to the following projects to assess expertise, quality of work and perceived competency in the context of the work contained in the RFO.

### 7.2. Project 1: Design and Implementation of Advanced Security Analytics, Insights and Alerts

(a) DIR wishes to identify, design, implement, and deploy an Enterprise Level Security Analytics, Insights and Alerts detection capability, initially focused on matters complimentary to the scope of this RFO, but with the capability for DIR to be able to extend the service to other generalized uses in the State's IT applications and infrastructure portfolio. The proposed solution should be complimentary to existing State capabilities including but not expressly limited to infrastructure level security and

protection of computing assets and facilities including but not limited to centralized intrusion detection, reporting, notifications, as well as network level protections around State firewalls, Web Application Firewalls (WAFs), network access/egress points, web servers, load balancers, hardware, servers, networks, storage, etc.

(b) Therefore, Successful Respondent must propose a Service (or framework of systems comprising an overall solution) that addresses all requirements in this Section, and if approved by DIR, implement specific capabilities as defined and required in this Exhibit.

### 7.2.1. Programmatic Security Access Detection and Analytics

(a) The Successful Respondent must specify, design, implement, and deploy a system to programmatically identify inappropriate access, intrusion, or suspected attempts at access that runs as a real-time background processes (transparent to users) that utilizes all available (both State and External Sources) contextual attributes and data points such as geolocation, device characteristics, user behavior, navigations and transaction activity to determine the likelihood of inappropriate access.

(b) The system will compare this information to expected behavior using machine learning or statistical algorithms, or State-defined or Successful Respondent proposed “best practice” rules that define “abnormal” access behavior and activities.

(c) The system will verify legitimacy of a user’s attempted access and infrastructure use using available internal and external information sources including the comparison of incoming identity information and contextual attributes (as described above) and comparing against available external and internal information (as required).

### 7.2.2. Identifying and Remanding Fraudulent, Inappropriate, or Suspicious Access Attempts and Other Methods

(a) The Solution must include, and be designed, implemented and deployed to leverage a combination of tools, rule-based (State and Industry Best/Common Practice) methods, Successful Respondent staff and processes as well as statistical or machine learning techniques to enable the linkage and relationships across users and other entities and their attributes using multivariate data stores to detect inappropriate access.

(b) The Solution must include, and be designed, implemented and deployed to analyze and correlate compute, network, user and other entity behavior across different access channels, modes and devices, and categorize alerts and warnings using a combination of State and Best/Common practices, rules and statistical methods.

(c) The Solution must include the capability to be extended to monitor and analyze compute, network, user and entity behavior as well as to identify anomalous or inappropriate compute, network, user or entity behavior using a combination of State and Best/Common practices, rules and statistical methods.

(d) The Solution must be designed, implemented and deployed to:

(i) Detect account takeover, which can occur when user account credentials are stolen (e.g., via malware-based attacks);
(ii) Detect repeated or systemic attempts at password hacking, denials of service (distributed or otherwise) or other means to circumvent, suspend, bypass, breach or render unusable DCS infrastructure assets inclusive of web, application, database applications as well as network level devices such as firewalls, routers, load balancers, etc.;
(iii) Identify and detect automated scripts targeting networks, accounts or a DCS Customer system or infrastructure asset;
(iv) Identify and detect automated scripts engaged in a massive attack against a large number (e.g., hundreds or thousands) of infrastructure elements, systems, and accounts;
(v) Identify and detect attributes pertaining to an individual conducting a manual or coordinated attack (e.g., source, IP address(es), country, location and other identifying attributes) to assist the State in both protections from the attack as well as pursuing additional means to reveal the origin/source of the attack;
(vi) Identify and detect a combination of human(s) and automated script(s) executing either targeted or mass attacks; and
(vii) Identify and detect fraudulent or suspicious access via location based, network, device, browser or other methods that are inconsistent with authorized legitimate access.

(e) The Proposed Solution must support user and entity profiling and behavioral analytics, such that a user's or entity's ongoing behavior is captured in a profile that can subsequently be used to compare against new activity to determine whether the activity is legitimate.

(f) The Proposed Solution must include anomaly detection capabilities using statistical models, rules, or a combination of both. Ideally, one or more of each type of statistical model must be supported by the Solution for State use.

(g) Solution modeling capabilities must include:

(i) Confirmed “bad” behavior and access methods that indicate illegitimate access;
(ii) "Normal behavior," most of which is assumed to be "good,” including common system uses, navigation transactions, transaction limits, historical transaction levels and values and other factors;
(iii) The Solution should, as part of routine functions establish a history of confirmed fraud and bona-fide use, and include baselining various activities and entity behaviors;
(iv) Detection of anomalies that deviate from established baselines but include controls to help the State to manage transactions holistically realizing that not all anomalies represent intrusion or attempts to deny service through any means;
(v) Continuous behavioral profiling of computing assets, networks, traffic, accounts and entities;
(vi) Ingesting and integrating external threat intelligence into intrusion detection analysis and operations, initially from DCS Enterprise tools;

(vii) Using the above data sources and other State data to compare incoming traffic or transactions across online channels with existing profiles and norms of user or entity behavior in order to detect intrusions or denials of service; and

(viii) Establish linkages and correlations between fraud detection uses rules, statistical models or both and linkages across key attributes, such as device, name, IP, phone, address and email address and other factors, to find patterns of suspect activities.

(h) The Successful Respondent is responsible for an overall solution design narrative that identifies the people (roles), process and technology the Successful Respondent proposes to use to meet the required outcomes articulated in this section to include:

(i) Overall solution design;

(ii) Detailed cost estimate;

(iii) Project development milestones; and

(iv) Estimated Project delivery timeframe (length of time to implement).

## 7.3. Project 2: Implementation of a DCS Identity and Access Management (IAM) Platform

### 7.3.1. Project Summary Objectives

(a) The summary objectives of this project are in light of increasingly public breaches of data from public and private institutions. The initial scope includes the systems and users of the DCS program and DCS systems hosted in the Consolidated and Non-Consolidated data centers, or in the Public Cloud. Texas.gov application-level services are excluded from this scope.

(b) The goal of this project is to:

(i) Establish and thereafter maintain a process for the DCS to validate DCS SCPs that access DCS infrastructure elements (collectively compute, storage networking, database, middleware and ancillary elements) whether in the DCS private cloud or in a public cloud provider.

(ii) Ensure that the service directly aligns with and supports the operations contained within DCS as they are required to drive highly trusted access to DCS systems and infrastructure and service elements in creating, establishing and maintaining Identities within DCS that includes design considerations to reduce or eliminate these Identities being compromised or used for fraudulent or not-authorized purposes by any party.

(iii) Develop a set of Enterprise Frameworks that address the variety of risk profiles associated with accessing State systems (e.g., accessing sensitive data, routine administrative systems use, accessing high risk data types such as those that contain personal, private, confidential or monetary/financial details).

(iv) Migrate DCS critical systems access for DCS SCPs and associated Privileged Users to a seamless two-factor ID Authentication and Accounting environment that move away from a login/password paradigm to a trusted and validated operation that reduces risk. Option to allow this to be extensible to DCS Customer accounts.

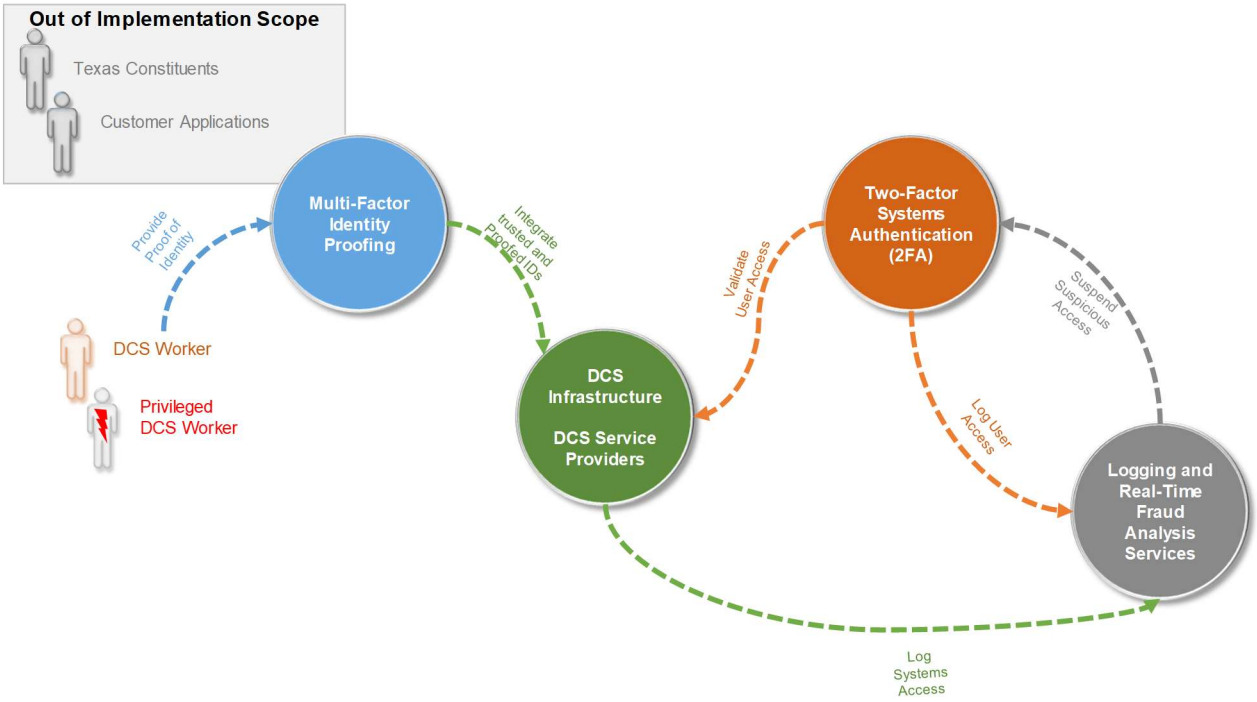
(v) Implement and operate the above capabilities in a phased approach that demonstrates end-to-end capabilities for all DCS environments.

(vi) Develop a process to deploy the solution as an Enterprise IAM Service for DCS Customers to purchase.

### 7.3.2. Conceptual Organization of Requirements

This Project includes providing an IAM solution for DCS SCPs. Texas constituents and customer applications are out of scope for this project's initial implementation. However, the IAM solution should be designed such that it can be later extended to customer applications. Pricing for customer application IAM will be determined after Commencement, at such time that DIR decides to offer this IAM service for customers to purchase.

**Figure 1: Conceptual Organization of Relationships of Requirement Areas in this Project**




### 7.3.3. Enterprise Architecture and Integration Standards and Conventions

#### 7.3.3.1. DCS Middleware Service Bus

Customer systems and systems architectures have been built over the years with a variety of middleware or service bus architectures. For purposes of this Project and general Enterprise use across DIR, Successful Respondents shall base their solution on the assumption that DCS Middleware, SOA, Web Services (in general) are prominent service bus architectures that will require interoperability and integration to the Enterprise offering and as such are acceptable and preferred unifying technologies for this DCS offering.

#### 7.3.3.2. Existing Directory Services

DIR's directory for general and administrative purposes (e.g., email, productivity and general identity purposes) is Microsoft Active Directory. In addition to system specific identity stores, there are significant concentrations of IBM/Tivoli, LDAP and other common directories and protocols.

#### 7.3.3.3. Existing Cloud Services and Systems

Texas has based several service offerings and has active development on a number of Cloud Based Services and Systems. Most prominent, and therefore required as a demonstrated factor in the overall solution are: VMWare (State cloud provisioning, orchestration and management); Salesforce.com; ServiceNow (enterprise IT service management, delivery and billing); and Microsoft Office365 (applications, productivity, email).

#### 7.3.3.4. Emerging Cloud Services

DIR continuously reviews the merits and use of a variety of Cloud based system and service offerings. Successful Respondents should indicate what parties and mechanisms their solution supports (generically) standard two (2) factor authentication using open TOTP standards or extensible to proprietary solutions such as Amazon AWS MFA, Microsoft Azure MFA, Google Authenticator, OpenID (e.g., Google, PayPal) or other ICAM or Federal Bridge/FICAM Certified Providers of Token Management and Authentication Services.

#### 7.3.3.5. Mobile Interoperability and Emerging Biometrics

DIR acknowledges the increasing importance of mobile devices across DIR and by our constituents. Many of these devices maintain provisions for two (2) factor biometric based authentication such as Apple iDevice based TouchID, Android based Fingerprint, Microsoft FIDO and other emerging standards. Successful Respondents should indicate who and through what devices and mechanisms that their solution supports two (2) factor authentication using mobile devices and computing platforms that offer similar biometric (fingerprint, voice and IR image) based factors.

#### 7.3.3.6. General Enterprise User Counts and Sizing Considerations

Successful Respondents are to design and implement the proposed systems to directly support the sizing required in the Privileged Access Management requirements, but be capable from an architectural/sizing perspective to scale to address the following **approximate** populations:

(i) Internal to DCS: 2,000;
(ii) State Agencies (if all Customer Agencies adopt IAM for all their applications): 150,000;
(iii) As part of the work the Successful Respondent will address Enterprise Identity Interoperability Standards:
   A. Use of State Standard Enterprise Service Bus Architectures and Elements;
   B. Use of State Enterprise Active Directories and Customer/Application Specific Identity Stores;
   C. Federation and Trust Frameworks;
   D. Use of 3rd Party Cloud Software Directories and Federation Method(s); and
   E. Mobile Interoperability Standards.
(iv) Sizing and Scalability Requirements and Considerations.

### 7.3.4. Enterprise Directory Support

(a) LDAP v3 inclusive of Application Program Interface (API) calls:

(i) IBM/Tivoli Single Sign On;
(ii) Microsoft Active Directory (all OEM Supported Versions);
(iii) External radius server;
(iv) Two-factor authentication;
(v) Novell IDM v3.5 or higher;
(vi) User ID and Passwords;
(vii) State Provided Access control lists and files: and
(viii) Future industry standards.

(b) The System should consider the use of the following two-factor authentication (2FA) methods:

(i) Biometrics;
(ii) Directories;
(iii) Smart cards;
(iv) Tokens;
(v) Public Key Infrastructure (PKI) and Certificates;
(vi) Voice recognition; and
(vii) Shared secrets.

(c) As part of the work the Successful Respondent will address the Enterprise Identity Directory Support Capabilities inclusive of:

(i) Use of Existing Directory Stores;
(ii) Master Directory Federation Strategy;
(iii) Integration Methods;
(iv) Legacy Directory Retirement/Replacement Strategy and Checklist;
(v) Published APIs and Integration Method(s);
(vi) Identity Provisioning; and
(vii) Audit and Logging Capabilities.

### 7.3.5. APIs, Workflow and State Development Tool Support

Successful Respondents must identify, select and propose a Solution that meets the following requirements at a minimum, should a Successful Respondent solution exceed these standards, Successful Respondents should highlight the perceived merits, rationale and (if applicable) limitations of the proposed solution:

(i) The solution must provide a clear development path for allowing DCS Customers to integrate their web-based applications for reverse proxy portal integration or equivalent functionality.
(ii) Integrate with the MSI service management system to support request management and user life-cycle workflows.
(iii) The solution must provide a Software Development Kit (SDK) for extensions surrounding workflow, custom provisioning, and triggers.
(iv) The solution must support the use of open source or well supported leading industry development tools, subject to State approval as well as support for integration with

State applications and services which support authentication methods that are LDAP and Active Directory capable.

(v) The solution must support both Java based development activities using J2EE and current supported JDK version and Microsoft Windows specific development using .NET based methods. Successful Respondents are to indicate any additional methods for Java and Windows specific development activities that DIR may utilize using the proposed solution.

### 7.3.6. Directory Services and Provisioning

(a) The system must support custom attributes of LDAP or Active Directory.

(b) The solution should be able to provision and de-provision identities in LDAP, non-LDAP, and Active Directory targets across the DCS enterprise.

(c) The solution shall not allow anonymous access to the production LDAP or Active Directory.

(d) The solution must provide the ability to support self-registration and user originated application requests with an approval queue for application administrators, if a DCS Customer chooses to extend the system to their employees.

(e) Solution must allow for self-requests for automated password reset where appropriate.

(f) Solution must support multiple workflow paths, depending on the type of user such as, but not limited to state employee, identified citizen, customized web experiences, etc.

(g) Solution must support the development of customized workflows.

(h) Solution must support notification workflow capabilities.

(i) The system should support workflow approvals from secure authorized mobile devices.

### 7.3.7. Audit and Logging Requirements

(a) The System must provide full and configurable auditing capabilities, including the creation/deleting of users, password resets, role/privilege assignment, token assignments, 2 factor method(s) and devices etc.

(b) The System must provide full auditing of access to applications, access to resources, and access to individual user accounts.

(c) All auditing logs must be reviewable by state security administrators and security policy staff using access to system logs and via the Programmatic Fraud Detection system(s) proposed by the Successful Respondent.

(d) The System must support real-time replication or integration of audit logs to the Security Operations Security Information and Event Management (SIEM) solution (currently McAfee) for audit reporting, alerting and management by Security and Privacy Personnel. Refer to Section 7.3.7 Audit and Logging Requirements.

(e) The system must be configurable for auditing events and be extensible to support situational analysis of events and breeches (active and retrospectively) as to support incorporation of new rules, methods, tools and techniques to further enhance DIR's overall security posture in the future.

(f) All system activity must be attributed and logged to a single, unique system user, identifiable by individual persons.

### 7.3.8. General Application Use and Integration Requirements

(a) The solution shall be capable of linking multiple customer third-party credentials to a single DCS identifier for the Customer.

(b) The solution shall be capable of presenting a DCS State identifier to a specific relying party, regardless of which third-party provider the Customer successfully authenticated with.

(c) The solution shall present Customers with an option to integrate Customer systems with those systems third-party credentials with their State unique identifier.

(d) The solution shall allow Customers to link multiple third-party credentials together into a single State identifier to access the same Customer.

(e) The solution shall allow Customers to unlink their third-party credentials from their State identifier.

(f) The solution shall allow customers to decline registration of multiple third-party credentials with DIR.

(g) The solution shall allow Customer to un-register their third-party credentials with DIR and destroy DIR identifier.

(h) The Successful Respondent will describe how tolerance levels are applied to the identity data elements. (e.g., married vs. single surnames, extra spaces, variance in address – street vs. avenue, etc.)

### 7.3.9. Customer Application Use and Integration Requirements

(a) While out of scope for the initial DCS implementation, the system (for future Customer use) must support application authentication and authorization by individual user. User account information must be stored securely in a database. Users may belong to multiple groups and roles.

(b) The application will enforce the DIR standards or specific Customer system requirements, whichever are more restrictive for individual passwords for allowable characters, length and expiration period.

(c) The application must follow the DIR standards or specific Customer system requirements, whichever is more restrictive, to lock out users after invalid login attempts.

(d) The application must provide the system administrators with the capabilities to define different roles with different privileges.

(e) The application will provide the system administrators with the capabilities to create groups whose members can be either role-based or individual login account names.

(f) The application will address Enterprise Application Use Standards inclusive of:

(i) Use of Existing Directory Stores;
(ii) Master Identity Federation Strategy;
(iii) Integration Methods;
(iv) Published APIs and Integration Method(s); and
(v) Audit and Logging Capabilities.

### 7.3.10. User Administration and Provisioning Requirements

(a) The proposed Solution will allow the ability for local State administrators with rights to add, disable, and modify users, if and when DIR extends this IAM service to Customers.

(b) The proposed Solution will allow users (e.g., SCPs) to centrally provision and de-provision; meaning accounts are enabled or disabled Statewide from the Successful Respondents identity vault.

(c) User and account provisioning and de-provisioning within the DCS Identity Domain (AD) will continue unchanged as a result of this Exhibit.

(d) The proposed Solution must support one identity per entity, with users possessing rights to multiple applications and resources. Users should have a single password with other factors such as PINS, tokens, biometrics, etc., as required. The same entity may have more than one identity depending on context.

(e) The system must provide central administration for manually manipulating identities, including password reset, user creation, granting roles/privileges, etc., and log all of these actions for auditing purposes.

(f) The system must have a single web and web service interface that allows for the management and administration of identity management systems.

(g) The system must have the ability to enforce password policies including:

(i) Expiration of passwords;
(ii) Challenge/response capabilities for forgotten passwords; and
(iii) Password strength policies.

(h) The system shall use preset values to reduce the time to create, provision, suspend and terminate an account correctly.

(i) The solution must support the ability to assign attributes based on the user's context (e.g., group membership, roles, permissions, etc.).

### 7.3.11. Single Sign-On Support

(a) The proposed Solution must include support for a reverse proxy access control or equivalent functionality, authenticating the user for all applications for which the user has been granted access.

(b) The proposed Solution must enable Single Sign-On (SSO) integration with the MSI's Portal.

(c) The solution must support integrated workflows to enable automated provisioning and de-provisioning based on feeds from authoritative sources.

(d) Solution must support delegated administration for applications accessible through the Successful Respondent portal.

### 7.3.12. Solution Administration Portal: Users, Relying Parties and DIR

(a) On user login, the Solution will support the ability to present a custom web portal to the user that shows systems to which the user has rights of access. This Portal:

(i) must be designed for multiple interfaces (desktop/laptop, tablet, phone);
(ii) must have the ability to allow/disallow users to modify the user's portal home page;
(iii) must have user's self-care capabilities, such as, but not limited to, user's changing passwords, challenge response and personal information;
(iv) must provide for System Administrators to post communications/notifications; and
(v) must allow dynamic additions and deletions of systems to the portal without impacting other systems.

(b) Administration of the Solution Portal:

(i) must provide configurable attributes by location, object classification, applications and other attributes;
(ii) must have a uniform interface across the Service Provider's solution for State Administrators;
(iii) must provide a web-based user interface for administrative tasks. Please describe the administrative tasks supported with and without a web-based user interface;
(iv) must provide role-based access control capabilities for administrators and administrative tasks;
(v) must enforce separation of duty (SoD) and operate on least privilege policy for administrator access; and
(vi) must provide a web-based user interface to manage third-party providers.

### 7.3.13. FICAM Compatibility and Evolution Currency

(a) The System shall support all currently approved FICAM Protocol Profiles for browser based SSO. (OpenID 2.0 and SAML 2.0 required; Identity Metasystem Interoperability version 1.0 (IMI 1.0) support is optional).

(b) The Successful Respondent shall provide a detailed plan for supporting any newly approved or future FICAM Protocol profiles within ninety (90) days of final approval by the ICAMSC. The implementation of any such plan must be approved by DIR and implemented by the Successful Respondent upon mutual agreement.

(c) The solution must be capable of supporting all FICAM Adopted Trust Framework Provider Approved Credential Providers.

(d) The solution must be capable of supporting PIV (for Government-to-Government use cases) and PIV-I Authentication. This support must include Trust Path Discovery and Trust Path Validation functionality.

### 7.3.14. Protocol Standards and Support

(a) If the Solution implements a SAML 2.0 Attribute Query/Response mechanism, it shall support the FICAM SAML 2.0 Identifier and Protocol Profiles for BAE v2.0 and the associated FICAM SAML 2.0 Metadata Profile for BAE v2.0.

(b) The Solution shall, at a minimum, support the following protocols and assertion formats for communication between itself and the relying party Customer application: Protocols: HTTP(S), SAML 2.0 and Assertion Formats: SAML 2.0, XML, JSON.

(c) The Solution must support full and policy or filtered interfaces with other directories, including at least Tivoli, Active Directory (AD), eDirectory and Lightweight Directory Access Protocol (LDAP) or equivalent Active Directory functionality.

(d) The Solution must provide support for a minimum of 256-bit TLS encryption for transport and must be configured to communicate using TLS/ SSL or other appropriate forms of encryption.

(e) The Solution must support strong one-way encryption (hashed) of passwords.

(f) The Solution must support Public key Infrastructure (PKI) where appropriate.

(g) The Solution shall support standard attribute sharing protocols including but not limited to:

- (i) SAML 2.0 (Mandatory); and
- (ii) OpenID 2.0 (Desirable).

(h) The Solution shall support the following for communications between itself and the relying party application:

- (i) ICAM SAML 2.0 Web Browser SSO Profile; and
- (ii) ICAM OpenID 2.0 Profile (Desirable).

(i) The Solution shall, at a minimum, support the following protocols between DIR and the PKI Certificate Authority but it is not limited solely to these:

- (i) OCSP over HTTP;
- (ii) CRL over LDAP and HTTP; and
- (iii) SCVP over HTTP.

(j) FCCX shall support HTTP/S protocols between DIR and a State Customer but not be limited to HTTP/S exclusively. Additionally, the Solution shall have the ability to integrate with additional protocols at State request.

### 7.3.15. System Auditing Requirements

(a) The Solution shall log and make available by reports and the Enterprise Logging, Audit and Fraud Detection capabilities contained elsewhere in this Exhibit all activities related to the:

- (i) Customer authentication request;
- (ii) Third-party provider authentication results;
- (iii) Assertion to a relying party;

(iv) Relying party attribute request;
(v) Attribute provider communication;
(vi) Customer account linking of third-party providers;
(vii) Changes in third-party providers;
(viii) Notification date and time stamps;
(ix) Onboarding and off-boarding of third-party providers;
(x) Onboarding and off-boarding of relying parties; and
(xi) Performance of Administrative functions.

(b) In addition to the above as a set of Administrative and Technical requirements, the solution shall:

(i) Allow administrators to view audit logs in a web user interface;
(ii) Store audit logs for a minimum of two (2) years with three (3) months of data online and readily available, nine (9) months of data available within twenty-four (24) hours, and the remaining twelve (12) months of data available for restoration within forty-eight (48) hours;
(iii) Support near real-time analysis of events;
(iv) Store all logs from all redundant instances of the service in a centralized database;
(v) Log activities related to notice and opt-in; and
(vi) Have the ability to define and configure logging activities including types of data and maximum storage time.

### 7.3.16. System Reporting Requirements

(a) The solution shall be capable of producing audit reports via either Successful Respondent provided web reporting tools or State access via State standard reporting tools.

(b) The solution shall have the capability to generate ad-hoc business reports that can support internal State invoicing needs including Customer use/consumption, application level access and proration of the entire Service based on Customer actual use/consumption.

(c) The solution shall be capable of producing a web accessible report dashboard with the ability to export the report in CSV, PDF and Excel as appropriate to the content of the report.

(d) The solution shall not display or maintain sensitive personal or financial information in logs or administrative messages.

(e) The solution shall be capable of generating a report for a specific customer pseudonymous identifier when the identifier is required to support other functionality.

### 7.3.17. Industry Compliance Requirements

(a) The solution shall be designed and implemented to become FISMA certified at moderate security category and plan to attain certification at DIR's direction and nothing provided by the Successful Respondent shall be designed, implemented or deployed as to preclude or confound such certification.

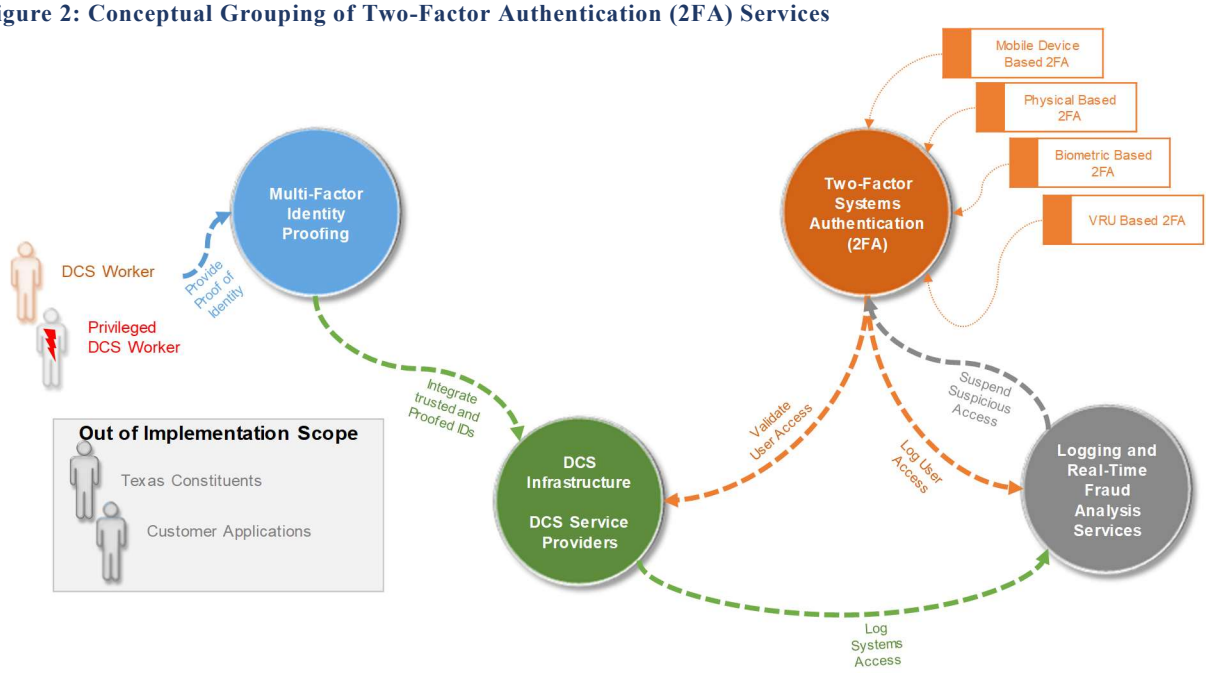
(b) If the IAM solution is public cloud hosted, then it shall be designed and implemented to allow DIR to consider FedRAMP certification in the future and in the interim comply with or exceed current FedRAMP requirements for a moderate system.

(c) The software solution shall be Section 508 compliant, see http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/guide-to-the-section-508-standards, for applicable definitions, standards, etc.

### 7.3.18. Two-Factor Authentication (2FA)

(a) Conceptually, these requirements can be viewed in the context of this overall Project as follows:

**Figure 2: Conceptual Grouping of Two-Factor Authentication (2FA) Services**




(b) The Successful Respondent is responsible for the specification, design, installation and configuration of a Third-party Two-Factor Authentication (2FA) service that includes Token Origination Services(e.g., the creation of a Token, either one-time, physical, device, or based), Token Authentication Services (e.g., validation of the authenticity of a user provided Token) and Token Management Services (e.g., cancellation, replacement or device based registrations) that will be used in integration with a State System and a user transaction to validate the authentication of authorized users within DCS (or a State system's) policy management capability.

(c) The two-factor authentication solution will be designed and implemented to require a user to provide two (2) unique factors: something they know, like a password or PIN, and something they possess like an authenticator, a hardware or software token with a code that changes randomly every sixty (60) seconds. This two-factor authentication must ensure that it is far more difficult for an unauthorized or illegitimate party to gain access to State system authentication credentials. DIR requires a solution based on the practicalities of supporting the general public that have a variety of capabilities including mobile based devices, Physical or Fob based, emerging biometric based (e.g., fingerprint, voice and IR imaging based) as well as voice response (VRU) based. The proposed

solution should support all methods mentioned above to provide DIR as much flexibility as possible to balance the practicalities, distribution and economics of this second factor with the relative risk profile of the interaction between a State system and a system user (e.g., Citizen, Business, Vendor, State Worker or Privileged State Worker) as appropriate.

(d) In general, these Services must be highly available and provide fully redundant and fully diverse network access and support DIR's multi-Customer, multi-system environment as well as emerging cloud-based offerings that DIR utilizes for Enterprise systems and services.

#### 7.3.18.1. User Authentication

(a) System must support LDAP and Active Directory calls for username and password authentication, including passing an encrypted password string.

(b) System must support integration with the proposed two-factor authentication services/solutions and/or adaptive authentication services/solutions as required, including at least RSA SecurID tokens or stronger similar physical tokens.

(c) System must support elevated (step-up) authentication, meaning that as a user requests more secure access, authentication requirements increase.

(d) System must support location sensitive authentication, meaning authentication requirements increase as users attempt to access resources from less secure locations.

(e) Solution must support Authentication and integration with the following technologies: Oracle DBMS, Microsoft SQL Server DBMS, DB2 for Z/OS DBMS, Windows Server, Linux, VMWare, Unix (generally AIX and HPUx) and to the extent possible support federated single-sign on or credential brokering of administrator authentication to an identity store, and the seamless logon to the technology where the administrator never knows the password.

(f) Solution must support password synchronization with the following technologies: Oracle DBMS, SQL Server DBMS, DB2 for Z/OS DBMS, Windows Server, Linux, VMWare, Unix, others.

(g) Solution must support temporary authorization of elevated privileges (such as granting domain admin to someone for a specific number hours to perform work, preferably from a known access location (e.g., IP address, VPN destination or PC/Mobile device) and then revoking the permission at the conclusion of the temporary period.

(h) Solution must include a web services interface, to be callable by external applications for use with application service accounts.

(i) The solution must be able to integrate with DIR's PKI for certificate-based authentication including support of revocation or suspension.

(j) System must provide mechanisms to prevent brute force attacks and other well-known attacks.

(k) Authentication must support operation as an HTML form in a browser without plug-ins or additional software, regardless of browser (currently OEM supported versions of Internet Explorer, Microsoft Edge, Firefox, Safari, Chrome) or device type (desktop, tablet, mobile phone) or operating system (OEM supported versions of Windows, Linux, Unix: AIX, HPUX, Android, or IOS).

(l) Supported User browsers must support HTTPS and session cookies.

(m) The System will address 2FA Integration Enterprise Standards:

(i) Determine Appropriate 2FA parameters for multiple types of Users.
(ii) Establish Operating Norms and Exception Policies (for onward Detection, Auditing and Tracking).
(iii) Document standards for integration for use by other systems.

### 7.3.19. Standards Compliance

(a) System must provide mechanisms for compliance with all State and Federal laws and mandates that DIR is subject to including, but not limited to HIPAA, CJIS, IRS Pub.1075 Et.Seq., Homeland Security, and PCI for access to and use of secure data and applications.

(b) System must support federated identity management, using NIST best practices and equivalent industry standards for interoperability and integration with external public and private institutions. Including, but not limited to the following sub sections of 15.2:

(i) System must follow NIST 800-53 control standards for secure access to data and systems.
(ii) Solution must integrate with any existing DIRs authentication system or provide NIST compliant advanced authentication per advanced authentication at level 3 or level 4 as defined in NIST SP800-63.

(c) As part of the work the Successful Respondent will incorporate Enterprise Identity Interoperability Standards inclusive of:

(i) Trust and Encryption Levels;
(ii) Mandatory Data Elements and Customer Specific Options;
(iii) Maintaining Public Privacy;
(iv) Private Data Handling and Disposal Standards;
(v) Data Physicalization and Duplication Standards; and
(vi) State Tolerance Considerations.

### 7.3.20. General Technical Requirements

(a) The system must support and be implemented with a failover configuration to ensure high availability.

(b) System must not have a single point of failure and must support full back up and restore capabilities so that the system can be restored from media with minimal additional intervention.

(c) The batch and backup operations must not degrade the response times of the system in off hours, assuming a lower request load to be estimated and justified by the Service Provider.

(d) The Successful Respondents hosted primary production and disaster recovery sites and all State data must be in the continental United States and located as to be technically diverse from the primary production site.

(e) Technical diversity factors include at a minimum: alternative and redundant power providers or grids, telecommunications network providers to those servicing the primary and disaster recovery sites respectively.

### 7.3.21. Performance and Scalability Requirements

(a) The system must support a minimum of 99.99% uptime for 24 x 7 x 365 operations and must support a peak load of twice (2x) the expected maximum concurrency to ensure adequate spare capacity for growth and expansion without an unacceptable degradation of performance.

(b) The initial maximum concurrency is 2,000 users, but the Successful Respondent is encouraged to adjust this number upward or downward with supporting data and estimation methods.

(c) The Successful Respondent and DIR will review actual peak load data no less frequently than twice yearly and mutually make sizing increase and deprecation decisions based on the actual load of the system.

(d) The Successful Respondent and State will review performance in advance of any such significant onboarding activity in the context of the then current performance and available capacity of the system and make adjustments as appropriate as to maintain a positive user experience from a performance and availability perspective and as to support ongoing attainment of Service Level Requirements.

### 7.3.22. Authentication/Access Reporting and Logging Requirements

(a) System must provide authentication and access reports based on any arbitrary attributes DIR requires as provided by the underlying software or solution elements.

(b) System must support report generation and logging to a State data store for administration tasks, including, but not limited to password resets, granting of privileges, account suspensions, and any other auditing event.

(c) System must support report generation and alerting of State Security personnel both directly and via the SIEM for Security Incidents such as, but not limited to, hacking attempts and attempts to access secure resources above an individual's access levels.

(d) The solution must support configuration of Standardized and ad-hoc reports without requiring any customized programming using common desktop reporting tools.

### 7.3.23. System Operational Reporting, Alerts and Notifications

(a) System must include real time mechanisms for monitoring responsiveness, resource consumption, storage utilization, and overall system health.

(b) System should include support for intrusion detection and other hacking attempts on identity stores.

(c) System must provide real-time notification to administrators and State monitoring staff for performance issues and any security event. Notification must be configurable for email, mobile phone, text messaging, etc.

(d) Alerts need to be configurable by administration staff, not requiring code changes.

(e) Follow a Master Monitoring and Detection Event Model by providing:

(i) Catalog of Suspicious and Fraudulent Behaviors
(ii) Tracking and Alerting Framework
(iii) Logging of Systems Access
(iv) Archive / Purge of Systems Access Logs
(v) Privacy Considerations in Event Logging
(vi) Integration with Enterprise Security, Notification, and Tracking Services

(f) Should the system determine that one (1) or more of: 1) a known fraudulent identity; 2) fraudulent activity; or 3) suspicious activity or transaction in progress the system will:

(i) Suspend access to the system, if actual behavior is out of range with what's expected or if the user appears suspect;
(ii) Remand attempted access to the system to DIR to conduct further manual review and investigation of the transaction or user, as warranted;
(iii) Trigger automated identity re-verification, stepped-up user authentication and/or transaction verification to automatically determine the legitimacy of the user or transaction as appropriate; and
(iv) Be configurable to initiate State (or DCS Customer) specific workflows related to suspending or if necessary terminating compromised accounts inclusive of (at DIR request) incorporating terminated account data into State Known Fraudulent Identity stores.

### 7.3.24. Fraudulent Identities and Entities in State Data Stores, Onward Sharing within the State Requirements

The proposed system will be designed, implemented and deployed to:

(i) Identify, for DIR review, all identities and entities that are determined via the methods, tools and techniques in this Project as well as any Successful Respondent provided means to be fraudulent, erroneous or suspicious;
(ii) Ensure that no identifying details such as personal or credential (e.g., password or token) information is included in any physical representations of data;
(iii) Upon State concurrence or approval, provide automated programmatic mechanisms to include these identities and entities in State Enterprise data stores for onward and subsequent State use;
(iv) Provide secure, audited manual entry capabilities to add, delete or modify any records that may have been inadvertently added to a fraudulent identity store as a result of any systemic, manual or other means; and
(v) Log all activities, programmatic, systemic or manual pertaining to any adds, changes, modifications or deletions of data in any State fraudulent identity store for State review and auditing purposes.

### 7.4. Project 3: Data Loss Prevention Monitoring Services

As an optional capability, the Respondent, as part of their proposal, and as Successful Respondent Performing the Service will specify, design and implement comprehensive Data Loss Prevention Monitoring Services for all DCS computing assets within the State's private cloud, and to the extent supported, within public cloud computing assets. Such Services will:

(i) Detect and intercept unusual or fraudulent activities associated with data in the DCS service assets;
(ii) Tune the solution to minimize or eliminate "false positives" while ensuring the true positives are treated appropriately;
(iii) Provide DCS participants alerts on this type of behavioral anomaly for action/response;
(iv) Support programmatic (i.e., automated) interception or suspension of the user session(s) and lock out the user(s) to prevent a breach or exfiltration of State data;
(v) Support the detection, neutralization, and elimination malware in DCS service platforms including providing the ability to detect, quarantine, and neutralize malware and malicious applications and system processes;
(vi) Detect and monitor unsanctioned cloud applications and platforms usage that may lead to data loss, and a weakened governance of State data. The solution must detect traffic and file uploads to these unsanctioned platforms and provide DCS participants data as to prevent and eliminate such uses;
(vii) Protect against leaks of State restricted information such as personally identifiable information (PII) or design diagrams containing sensitive/intellectual property (IP), as to reduce the chances of a data breaches and maximize compliance with Federal and State regulations as Payment Card Industry (PCI), Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA), IRS1075 and other restricted data types;
(viii) Aid investigation of suspicious users and incidents for any DCS participant, where the solution detects unusual or suspicious user activity or a data leak or malware incident, and provide an integrated response and investigation platform that allows for not just that includes reporting and trending of incidents in dashboards and data that can be queried.

## 8. DCS Governance Model

### 8.1. Introduction

(a) The Department of Information Resources (DIR) has established the owner-operator governance model for DIR's current shared technology services programs, which currently include:

(i) Data Center Services (DCS);
(ii) Managed Application Services (MAS);
(iii) Managed Security Services (MSS); and
(iv) Texas.gov.

(b) This model involves DIR and DCS Customers at all levels in governance decision making, including as representatives on all governance committees. The owner-operator model focuses on resolving issues at the lowest possible level and driving for consensus-based solutions. Where consensus cannot be reached, processes include an escalation path. For greater detail on the owner-operator governance structure; the roles and responsibilities to maintain working relationships between the MSI and other SCPs, and the service management process, see the data room.

(c) The Successful Respondent will participate and work within the DCS Governance model as it relates to the requirements the Contract.

## 8.2. Governance: Meetings

### 8.2.1. Governance

The parties shall comply with the governance and account management provisions set forth herein.

### 8.2.2. Meetings

During the term of this Agreement, representatives of the Parties shall meet periodically or as requested by DIR to discuss matters arising under this Agreement, including any such meetings provided for in the Transition Plan and the Service Management Manual. During the Transition Period, this may include meetings with DIR, the Incumbent Provider, and other DIR SCPs. Each Party shall bear its own costs in connection with the attendance and participation of such Party's representatives in such meetings.

### 8.2.3. Member Responsibilities

DIR has invested in the owner-operator governance model as a best practice to promote proactive problem solving and effectively engage DIR, DCS Customers, and SCPs in a collaborative decision-making model. The Successful Respondent is responsible for meeting the requirements of an SCP as they relate to the governance model. The shared responsibilities for DIR, DCS Customers, and SCPs include:

(i) Foster an environment of open and honest communications;
(ii) Actively participate in governance processes, including providing input to issue discussions;
(iii) Proactively enable communications distributed by DIR to enable effective issue resolution;
(iv) Collaborate proactively to identify, report, document, and resolve at the lowest possible level:
  A. Service delivery and performance issues;
  B. Security services program issues;
  C. Contract and financial issues;
  D. Invoice disputes; and
  E. Customer relationship and communications issues.
(v) Document escalated issues with an appropriate level of detail to ensure resolution;
(vi) Participate in the development of and compliance with governance process improvement; and
(vii) Actively participate in training provided by DIR and others regarding the contract, services, performance, and stakeholder responsibilities.

### 8.2.4. Membership

DIR and DCS Customers are members of all solution groups and committees. SCP and MSI representatives are fully participating members of the solution groups and committees, except for the Contract and Finance Solution Group where they participate by invitation and do not participate in decision making. On the BELC, SCPs and the MSI participate in solutioning and consensus decision making, but in the rare event that the BELC cannot reach a decision by consensus, DIR and DCS Customer members may vote to reach a decision.

### 8.2.5. DCS Customer Member Responsibilities

Each DCS Customer partner group selects its representatives for all committees and solution groups. These members represent all the customers in that partner group. Members are expected to be prepared before attending meetings which includes:

(i) Review all meeting materials in detail, especially partner agency comments, prior to committee meetings;
(ii) Leverage technical resources from DIR or DCS Customer organization to build solutions;
(iii) Facilitate effective communication and problem solving to promote resolutions;
(iv) Communicate with partner groups as needed to prepare to represent their perspectives in discussions (DCS Customer committee members); and
(v) Strive to effectively communicate positions of each DCS Customer (Customer committee members).

### 8.2.6. Partner Group Responsibilities

DCS Customers who are not on committees have responsibilities to support the process and communicate with their representative. These responsibilities include:

(i) Resolve operational issues at the lowest possible level through local interfaces with SCPs;
(ii) Actively participate in review of governance issues to be informed and serve as a substitute at a committee meeting if necessary;
(iii) Engage and communicate with partner group representatives to support effective representation, issue resolution, and solution development; and
(iv) Establish and maintain strong working relationships with partner group members.

### 8.2.7. DIR Responsibilities

DIR provides overall leadership and coordination for governance. In this role, DIR's additional responsibilities include:

(i) Facilitate governance committee meetings and activities, including providing organizational, logistical, and communication support to all committees;
(ii) Facilitate the issue management process, including developing an issue communication system giving all DCS Customers visibility into all issues;
(iii) Triage issues and attempt immediate resolution if possible, and route unresolved enterprise issues to appropriate governance committees for resolution;

(iv) Provide relationship management for customers including serving as a point of escalation for issue resolution;
(v) Interpret the Agreement from DIR's perspective;
(vi) Manage financial interactions, processes, and relationships with SCPs;
(vii) Manage communications;
(viii) Coordinate ongoing training related to Agreement changes, process changes, and New Services; and
(ix) Perform vendor management and compliance functions including development and execution of Agreement amendments.

### 8.2.8. SCP and MSI Responsibilities

(a) To enable the governance model, all SCPs have an important role as subject matter experts on technology, solutions, and feasibility. This includes the following responsibilities:

(i) Engage directly with DCS Customers to resolve their specific operational issues at the local level;
(ii) Assign empowered subject-matter experts to participate as requested in governance committees to resolve enterprise issues;
(iii) Research, as necessary, and document SCP perspective for issue resolution papers;
(iv) Provide timely and accurate data, information, and responses to promote prompt resolution of issues; and
(v) Enable and facilitate use of the issue management process.

(b) The MSI has additional governance responsibilities beyond those of the SCPs, including:

(i) Providing DIR with the operational intelligence to select appropriate topics, issues and opportunities for meeting agendas;
(ii) Preparing agendas and presentation materials; taking and posting meeting notes;
(iii) Coordinating issue escalation when multiple SCPs are involved;
(iv) Coordinating SCPs participation in governance meetings;
(v) Offering process improvement solutions to reduce the number of escalated issues;
(vi) Streamlining the issue escalation processes between SCPs;
(vii) Coordinating implementation of decisions and solutions that are approved by the governance committees; and
(viii) Posting all governance agendas, presentations, meeting notes, decisions and policies on the Portal.

## 8.3. Issue Management

(a) Governance committees address two (2) types of decisions:

(i) Issue resolution; and
(ii) Strategic decisions as per the roles and responsibilities.

(b) Escalated issues may be raised from a DCS Customer, SCP, MSI, or DIR. DIR identifies and presents strategic decisions to governance committees and solution groups. Both decision types are treated the same by the committees:

(i) All DCS Customers have an opportunity to hear the issue;
(ii) DIR performs triage and routes unresolved issues to appropriate committees;
(iii) All DCS Customers and all SCPs have an opportunity to provide their perspective to their partner group in advance of the meeting;
(iv) DCS Customer committee members will review partner group positions/perspectives to represent their partner entities in the meeting;
(v) All SCPs can present their position to the committee or solution group;
(vi) All decision-making agenda items will be broadcast in advance of the meeting; and
(vii) After the meeting, decisions will be documented with the issue.

### 8.3.1. Escalation Process

(a) As noted above, the governance model strives to resolve issues at the operational level. However, not all issues will be resolved at this level, so the governance model includes an escalation process designed to route the issue promptly and efficiently to the appropriate committee for resolution. Most operational issues will be routed to a solution group; however, the ITLC is the first resolver for high profile business, technology, and financial issues.

(b) After the DCS Customer and SCP determine an issue cannot be resolved at the local operational level, the issue is escalated to DIR. DIR triages and makes a further attempt to resolve. If resolution is not reached quickly, then DIR determines the appropriate committee for resolution and coordinates with the DCS Customer Committee chair or co-chair to determine when the issue can be placed on the agenda.

(c) DIR also coordinates with the DCS Customer and SCPs involved in the issue to complete the required documentation for DCS Customer input on the process as follows:

(i) DIR and the committee chair or co-chair coordinate the distribution of the issue material with the meeting agenda;
(ii) Meeting agendas and associated material are distributed to DCS Customer IT Directors in advance of the meeting, with approximately five (5) to seven (7) DIR Business Days for DCS Customers to review and provide input to their committee representative and approximately two (2) days for DIR to compile the comments received for distribution to all.

### 8.3.2. Notice by Successful Respondent

Without limiting its obligations under this Agreement, Successful Respondent shall expeditiously notify DIR when it becomes aware that an act or omission of DIR or DCS Customer personnel or a DIR Contractor shall cause, or has caused, a problem or delay in providing the Services, and shall work with DIR, the DCS Customers and the DIR Contractor to prevent or circumvent such problem or delay. Successful Respondent shall cooperate with DIR, the DCS Customers and DIR Contractors to resolve differences and conflicts arising between the Services and other activities undertaken by DIR, the DCS Customers and DIR Contractors.

### 8.3.3. Strategic Decision Process

(a) Strategic program decisions may be required by the Agreement (e.g., Technology Plan) and, thus, follow a prescribed timing cycle or they may arise from a technical constraint, opportunity or business need. Regardless of the source, strategic decisions follow a similar process:

  (i) DIR coordinates the development of background materials to explain the decision, implications for the enterprise, and any technical considerations that are relevant. This coordination may include the engagement of DCS Customer or SCP subject matter experts to create materials and complete technical analysis.
  (ii) DIR develops a format for DCS Customer input appropriate for the decision.

(b) DIR and the committee chair or co-chair coordinate the distribution of the issue material with the meeting agenda. Meeting agendas and associated material are distributed to DCS Customer IT Directors in advance of the meeting, with approximately five (5) to seven (7) DIR Business Days for DCS Customers to review and provide input to their committee representative and approximately two (2) days for DIR to compile the comments received for distribution to all.

### 8.3.4. Decision Documentation

After the committee meeting, DIR documents decisions made and any follow up tasks such as updates to associated artifacts (e.g., SMM). Decisions are posted to the Portal for visibility by all Authorized Users.

# 9. Cross-Functional Services

## 9.1. General Operating Model Requirements

(a) DIR contracts with multiple SCPs to deliver shared technology services to DCS Customers. Those services are integrated into a common service delivery model by DIR's MSI. The MSI provides the systems, processes and service delivery oversight necessary to ensure consistent, quality service delivery. The figure below depicts the future state relationships between SCPs and the MSI.

(b) DIR bases its Service Management practices on the Information Technology Infrastructure Library (ITIL), a world-wide recognized best-practice framework for the management and delivery of IT services throughout their full life-cycle. Accordingly, DIR requires that Successful Respondent Service Management practices, which are used to support the Services, be based on the ITIL framework and guidance as provided by the MSI.

## 9.2. Multi-sourcing Services Integration and Cooperation

Successful Respondent acknowledges and agrees that it will deliver the Services to DIR and DCS Customers in an environment in which there are various SCPs providing related services to DIR and DCS Customers ("Multi-sourcing Services Environment"). Successful Respondent acknowledges that its provision of the Services in a multi-supplier environment requires significant integration, cooperation, and coordination of processes and procedures with other SCPs. **Attachment 1.3 Service Level Definitions and Performance Analytics** specifies certain Service Levels and obligations to DIR and DCS Customers related to the provision of the Services in a multi-supplier environment.

## 9.3. Shared Technology Services Documentation Requirements – Service Management Manual

(a) All documentation maintained by the Successful Respondent shall be subject to approval by DIR and will conform to the documentation standards and format provided by the MSI and agreed upon between DIR and the Successful Respondent. The Successful Respondent shall develop documentation in accordance with this section. All documentation must be posted and maintained on the MSI-managed DCS Portal.

(b) The Successful Respondent shall, at a minimum:

(i) Ensure that Successful Respondent's operational procedures and documentation related to the Services is up to date, accurate, and posted on the MSI's Portal.
   A. Link Systems documentation to architectural standards;
   B. Identify DIR Data to the associated System(s) and the associated security risk classification; and
   C. Provide architecture and design documentation for Systems and Services managed by Successful Respondent.

(ii) Develop and maintain documentation on all Operations procedures, Services, Equipment, and Software for which Successful Respondent is responsible. Documentation shall be based on ITIL guidance to enable consistent management of process-driven IT services across a variable number of environments and among DCS SCPs.

(iii) Make all documentation available electronically on the MSI portal.

(iv) Validate documentation annually for completeness and accuracy in accordance with MSI SMM review cycle, and verify that all documentation is present, organized, readable, and updated in accordance with agreed upon schedule.

(v) Participate in MSI review of operational documentation validation, including reporting any findings to DIR and DCS Customers on a scheduled basis. Where it is determined that documentation is inaccurate (e.g., erroneous or out of date), correct and replace such documentation.

(vi) Update the SMM according to schedule described for the Critical Deliverables.

(vii) Ensure that ITIL-based processes effectively integrate with the processes, functions and roles deployed within and used by DIR and DCS Customers and other DCS SCPs. Develop and support required Application Program Interfaces (APIs) to integrate and automate provisioning, automated build, and decommissioning activities.

(viii) Design processes to enable the effective monitoring and reporting of the IT services in a Multi-Supplier Environment.

(ix) Ensure that enterprise processes (e.g. Change Management, Configuration Management, Problem Management) are followed across the DCS SCP and Third Party Vendor(s) processes.

(x) Coordinate the execution of all the processes across the Successful Respondent, DIR, DCS Customers, and all SCPs in order that all the individual components that make up the IT Services are managed in an end-to-end manner.

## 9.4. Marketplace and Portal Requirements

(a) The Successful Respondent must leverage the MSI-provided Portal (Portal) to provide integrated DIR and DCS Customer solutions, communications, and reporting. Reporting functions and specific operational reports are defined in **Appendix A Reports**.

(b) The Successful Respondent shall, at a minimum:

(i) Follow established MSI policies and procedures to ensure secure access to the MSI's DCS Portal, including identifying and working with MSI to resolve access issues;

(ii) Provide the MSI via direct data feed or system integration where possible with the reports and communication content to be posted, including but not limited to the following:

A. Processes
B. Documentation
C. Reports
D. Operational intelligence
E. Portal broadcast communications
F. DIR Shared Services tool links
G. Information pertaining to the delivery of Services

(iii) Develop and support Marketplace capabilities with API and automation to provide Customers with the ability to integrate and automate provisioning, automated build, modification, and decommissioning services and technology;

(iv) Provide reports and communication content in the format and design standards required of the MSI's online portal, and validate that content has been posted via MSI-provided secure access to the Portal;

(v) Leverage the Portal to access, update, and maintain DIR Shared Services documentation, including the following:

A. SMM;
B. Enterprise Policies;
C. Knowledge objects of Services;
D. Known errors and workarounds;
E. Training content;
F. Service Offering descriptions
G. Frequently Asked Questions (FAQs); and
H. Similar documentation for the Successful Respondent's organization as well as from other SCPs as specified by DIR.

(vi) Adhere to established policies, procedures, and processes as documented in the SMM.

## 9.5. MSI Tools and Operating Environment

(a) The MSI provides a digital tool and integration platform for all DCS and Shared Services providers to utilize in the delivery of services to Customers. Conceptually, this platform is as follows:

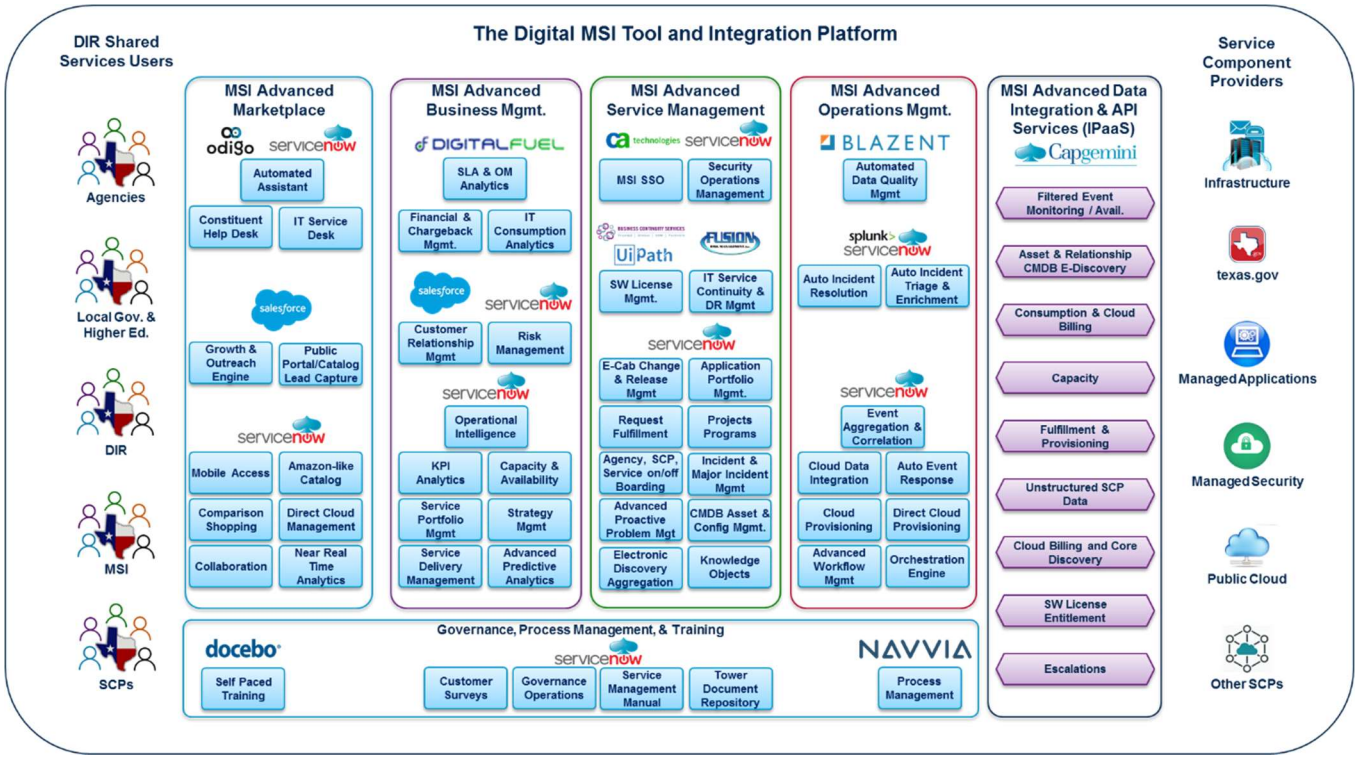



**Figure 3: Conceptual Diagram of the Digital MSI Tool and Integration Platform**

(b) The foundation of this platform is the ServiceNow cloud-based platform which delivers on the requirements of DIR and the MSI and provides efficient scalability and flexibility to serve the State of Texas.

(c) Beyond ServiceNow, leading toolsets are used to fill in functions that are not currently resident in the ServiceNow platform directly to offer a complete operating environment that is based on ITIL and ITSM standards. This platform will continue to evolve in a plug and play fashion for the foreseeable future.

(d) The MSI toolset also includes:

(i) **SalesForce.com** as the primary platform for the new DIR Growth and Outreach function;

(ii) **Odigo** for the IT Service Desk and the new Citizen Help Desk Automation associated with Texas.gov and future "citizen centric" services;

(iii) **Digital Fuel** for Financial Management, Chargeback, and SLA Reporting;

(iv) **CA Technologies** for the Digital MSI SSO Identity and Access Management Services;

(v) **BCS and UI Path** for Software License Compliance functions;

(vi) **Blazent** for Data Quality Management;

(vii) **Splunk** to capture un-structured data primarily from SCPs to aid in analysis and to use for Machine Learning data sets for identifying patterns that can be indicators of future incidents or outages;

(viii) **MSI-specific IPaaS** which will serve as the integration platform as an enabler for deeper and faster API integration with SCPs;

(ix) **Docebo** as the Learning Management Platform for the Digital MSI education functions;
(x) **Fusion Risk Management** for Disaster Recovery enablement; and
(xi) Risk Management within the portal serves as a vital management approach for the overall Program, through identification and management of risk mitigation.

## 9.6. Service Catalog Management

The MSI provides the Service Catalog tool for DCS Customers to request Services from the Successful Respondent. The Successful Respondent shall, at a minimum:

(i) Coordinate with the MSI to ensure automated integration of Successful Respondent Services into the Service Catalog, including integrating Successful Respondent fulfilment system with the Service Catalog (if applicable);
(ii) Work with the MSI to categorize and normalize Service Catalog content, including the following:
  A. Type of service;
  B. Configuration type
  C. Equipment or software type; and
  D. User eligibility in order to enable multiple selection, searching, and presentation views;
(iii) Work with the MSI to document and update Service descriptions and dependencies;
(iv) Participate, through the MSI, in regular communications with DIR and DCS Customers on updates to the Service Catalog; and
(v) Respond to Service Catalog requests in accordance with defined processes and Service Level Agreements (SLAs).

## 9.7. Customer Satisfaction Surveys

(a) The MSI will have responsibility for coordinating the development, maintenance, and execution of the surveys with DIR within the established Governance model. The MSI will develop the mechanism, facilitate responses, tabulate results and report results back to DIR and DCS Customers as part of an ongoing program for measuring customer satisfaction.

(b) DIR will have ownership of the overall review and approval of the customer satisfaction survey process, to include input and approval of the survey recipients, the survey methodology, and the survey questions.

(c) The Successful Respondent shall work with the MSI in developing, delivering, reporting, and tracking customer satisfaction. The SCPs shall support the MSI in accordance with the established SMM and **Attachment 1.1 Deliverables**.

## 9.8. Service Management Requirements

(a) DIR requires that the Successful Respondent follow design and implementation principles which will continue DIR use of ITIL compatibility. It is therefore required that the Successful Respondent design and deliver services via a set of ITIL compatible concepts and techniques for managing the DCS

private cloud and computing environment and integrate service management and reporting via the MSI operating model and systems.

(b) Respondents are advised that the DCS team and Customer-facing functions have been operating under and have been trained on ITIL principles and processes through the MSI's training program. Therefore, Respondents are not required to propose ITIL training as part of their response.

(c) The Successful Respondent will design and implement the Service as to ensure that the appropriate Service elements both integrate with and enable the following areas:

(d) The MSI Service Desk handles all in scope services incidents, problems and questions as well as providing an interface for other activities such as:

(i) Change requests;
(ii) Maintenance contracts;
(iii) Software licenses;
(iv) Service level management;
(v) Configuration management;
(vi) Availability management;
(vii) Financial management;
(viii) Application management; and
(ix) IT Services continuity management for DCS scope elements of this Exhibit.

### 9.8.1. Incident Management

(a) **Security Incident Management** process and procedures must be established as part of Service transition and commencement and thereafter continually refreshed according to the SMM currency process in order to have the capability to restore a normal service operation as quickly as possible and to minimize the impact on business operations. The objectives of the incident management process are to:

(i) Restore normal operations as quickly as possible with the least possible impact on either the business or the user, at a cost-effective price; and
(ii) Maintain a comprehensive inventory of 'known problems' (without a known root cause) or 'known errors' (with a root cause) under the control of Problem Management and registered in an error database.
(iii) The Successful Respondent will design and implement Security monitoring and oversight processes and procedures that include:
A. Incident detection and recording;
B. Classification and initial support;
C. Investigation and diagnosis;
D. Resolution and recovery;
E. Incident closure; and
F. Incident ownership, monitoring, tracking and communication.

(b) Successful Respondent shall, at a minimum:

(i) Provide Incident Management Services in the form of tier 2 support and tier 3 support. Incident Management is separate and distinct from Security Incident Management.
(ii) Provide knowledge capture and transfer regarding Incident resolution procedures to support the objective of increasing the number of Incidents capable of being resolved by tier 1 support.
(iii) Comply with MSI policies and procedures for Incident Management as documented in the SMM.
(iv) Coordinate with the MSI to develop and approve Successful Respondent-related Incident Management content in the MSI-managed SMM.
(v) Utilize the Incident Management System provided by the MSI for all information related to an Incident.
(vi) Provide for training on processes and tools for Incidents and escalations to Successful Respondent Incident Management staff and other relevant resources involved with responding to Incidents.
(vii) Resolve Incidents in accordance with the SMM, knowledge database documents, and configuration database(s).
(viii) Identify and classify Incident severity and handle according to agreed-upon Incident response procedures and assume end-to-end responsibility.
(ix) Escalate Incidents in accordance with the SMM, knowledge database documents, and configuration database(s).
(x) Provide tier 2 support and tier 3 support, unless tier 3 support is provided by a third-party vendor.
(xi) Participate in Incident review sessions.
(xii) Update the progress of an Incident's resolution within the MSI tracking systems through to final closure.
(xiii) Verify that all records (e.g., inventory, asset and configuration management records) are updated to reflect completed and resolved Incidents.
(xiv) Document solutions to resolved Incidents in MSI-managed central knowledge base. Accurately update all information pertinent to trouble ticket including general verbiage, codes, etc.
(xv) Determine if an Incident should initiate a Problem investigation (e.g., whether preventive action is necessary to avoid Incident recurrence) and, in conjunction with the appropriate support tier, raise a Problem record to initiate action.
(xvi) Conduct follow-up with DCS Customer representative who reported the Incident to verify the Incident was resolved to their satisfaction.
(xvii) Integrate the Successful Respondent's Incident Management process with the other service management processes, especially Problem Management, Configuration Management, Service Level Management, and Change Management.
(xviii) The Successful Respondent shall utilize the Incident Management System provided by the MSI and integrate such with their Incident Management processes, providing a level of detail that allows for a set of Incident Resolution diagnostics.
(xix) The MSI will provide the systems, processes and service delivery oversight necessary to ensure consistent, quality service delivery.

### 9.8.2. Problem Management

(a) **Security Problem Management** processes and procedures must be established as part of Service transition and commencement and thereafter continually refreshed to identify record, track, correct and manage problems impacting DCS service delivery. This area will be maintained to assist the State in recognizing recurring problems, addressing procedural incidents and containing or minimizing the impact of problems that occur. The Successful Respondent will support and follow established Problem Management processes to allow the State to find and resolve the root cause of incidents to minimize the adverse impact of IT infrastructure incidents and problems on the State and to prevent recurrence of incidents related to these errors.

(b) The objectives of the Security Problem Management process are:

- (i) Allow DCS to reduce the number and severity of incidents and problems on the business, and report it in documentation to be available for Service Desk agents and end-users; and
- (ii) Allow DCS to provide a proactive process that identifies and resolves problems before incidents occur.
- (iii) The Successful Respondent will design and implement processes and procedures that include:
  - A. Problem identification and recording;
  - B. Problem classification;
  - C. Problem investigation and diagnosis;
  - D. Identification of the root cause of incidents;
  - E. Trend analysis;
  - F. Initiation of targeted support action;
  - G. Providing information to the organization; and
  - H. Iterative processing to diagnose known errors until they are eliminated by the successful implementation of a change under the control of the Change Management process.

(c) The Successful Respondent shall, at a minimum:

- (i) Provide Problem Management Services in coordination with the MSI Problem Management structure to minimize the adverse impact of Incidents on DCS Customer's business operations.
- (ii) Cooperate with the MSI to provide reactive Problem Management Services by diagnosing and solving Problems in response to one or more Incidents that have been reported through Incident Management.
- (iii) Provide proactive Problem Management to identify and solve Problems and known errors before Incidents occur, including:
  - A. performing predictive analysis activities, where practical, to identify potential future Problems,
  - B. develop recommended mitigation plans, and
  - C. implement approved corrective mitigation actions and processes.
- (iv) Maintain, update, and disseminate information about Problems and the appropriate workarounds and resolutions to reduce the number and impact of Incidents.

(v) Provide Problem Management Services for all Problems that are determined to be related to the in-scope Services. Successful Respondent shall also provide coordination and assistance to DCS Customer and other SCPs in performing their Problem Management functions related to the in-scope Services.

(vi) Implement resolutions to Problems through the appropriate control procedures, especially Change management, as well as coordinating Problem Management activities with the various teams within Successful Respondent, DCS Customer, MSI and other SCPs responsible for performing Configuration Management, IT Service Continuity Management, and Service Level management activities.

(vii) Coordinate with the MSI to develop and implement processes for Problem Management and root cause analysis (RCA) (e.g., events that trigger an RCA).

(viii) Comply with MSI policies for Problem Management and RCA.

(ix) Participate in Problem Management review meetings.

(x) Use and update the Problem Management knowledge database managed by the MSI.

(xi) Perform Problem Management activities as set forth in the MSI-managed SMM.

(xii) Coordinate and take responsibility of Problem Management activities of all Problems that reside in Successful Respondent's area of responsibility (e.g., detection, logging, RCA, etc.).

(xiii) Conduct proactive trend analysis of Incidents and Problems to identify recurring situations that are or may be indicative of future Problems and points of failure.

(xiv) Develop and recommend corrective actions or solutions to address recurring Incidents and Problems or failures, as well as mitigation strategies and actions to avert potential Problems identified through trend analysis.

(xv) Identify, develop, document (in the MSI Problem Management tool), and recommend appropriate workarounds for known errors of unresolved Problems and notify Incident Management and all other appropriate DCS Customer stakeholders of its availability, if approved by DCS Customer.

(xvi) Create documentation with recommended corrective actions to resolve a Problem and submit to Change management for review and approval using the MSI provided tool.

### 9.8.3. Change Management

The Successful Respondent shall, at a minimum:

(i) Perform Change Management Services utilizing standardized methods and procedures as defined in the SMM to provide efficient and prompt handling of all Changes.

(ii) Assist DCS Customer in creating the schedule for any Changes and implementing such Changes.

(iii) Assist DCS Customer and MSI to refine and improve upon Change Management processes and training requirements including CAB composition, activities, and the financial, technical, and business approval authorities appropriate to DCS Customer requirements.

(iv) Comply with MSI Change Management processes and training requirements.

(v) Review and approve refinements to Change Management processes and training requirements.

(vi) Provide necessary information to DCS Customer and MSI to assist in documenting all Requests for Change (RFCs), which could include Change cost, risk impact assessment, and system(s) security considerations.

(vii) Coordinate with DCS Customer to assist in the development of a schedule of planned approved Changes.

(viii) Perform maintenance during regular Maintenance Periods as defined in the SMM, or as scheduled in advance with the approval of DCS Customer.

(ix) Provide Change documentation, as required, to the MSI, including proposed metrics on how effectiveness of the Change might be measured.

(x) As requested, participate in traditional or digital CAB meetings and workflow to review planned Changes and results of Changes made.

(xi) Utilize the Change Management System, tools, and processes of the MSI for the efficient and effective handling of all Changes, including the CAB, subject to approval from DCS Customer, in a way that minimizes risk exposure and maximizes availability of the Services.

### 9.8.4. Configuration Management

(a) The Successful Respondent will perform Configuration Management to provide a logical model of the IT infrastructure managed by the Successful Respondent to identify, control, maintain, and verify information related to all Configuration Items that enable the Successful Respondent's Services. The MSI consolidates information from multiple SCP Configuration Management Databases (CMDBs) that contain details of CIs used in the provision, support, and management of IT services.

(b) The Successful Respondent shall, at a minimum and as defined in the SMM:

(i) Actively participate with the MSI to develop and document Configuration Management processes, as approved by DIR, that document the objectives, scope, and principles that ensure the success of the Configuration Management processes.

(ii) Integrate Successful Respondent's Configuration Management process with the MSI's Configuration Management process and systems, including providing Successful Respondent Configuration data electronically to MSI's Configuration Management System (CMS) / CMDB in the agreed data format.

(iii) Communicate and coordinate the Configuration Management processes and policies within its organization.

(iv) Actively cooperate in information exchange between and among the SCPs, MSI, DIR and DCS Customer to improve end-to-end Configuration Management.

(v) Work with the MSI to provide a complete Configuration Management audit trail to meet DIR and DCS Customer legislative and policy requirements.

(vi) Conform operations to policies and procedures that set the objectives, scope, and principles that ensure the success of the Configuration Management process.

(vii) Work with the MSI in establishing categorization and classification structures to ensure the proper documentation and maintenance of CIs.

(viii) Use the Configuration Management process to identify, control, maintain, and verify the CIs approved by the MSI as comprising the Equipment, Software, and Applications to provide the Services.

(ix) Record all Successful Respondent's CI information including, but not limited to, equipment, software, software, services, and equipment.
(x) Verify that all CIs supporting the Successful Respondent's Services including Equipment, Software, and Services are incorporated into the CMDB.
(xi) Utilize the CMDB provided by the MSI as the single source of information regarding all CIs within Successful Respondent scope.
(xii) Ensure that all configuration data related to the Services resides in the CMDB.
(xiii) Integrate the Successful Respondent's other systems, including all appropriate and required licenses and/or interface with the MSI's Configuration Management System (CMS), as applicable.
(xiv) Where Successful Respondent has an internal CMS, integrate that system with the MSI CMS as required.
(xv) Where Successful Respondent has an internal CMDB integrate that database with the MSI CMDB.
(xvi) Provide customization as required to enable the Configuration Management processes as defined in the SMM.
(xvii) Automate processes, discovery tools, inventory and validation tools, enterprise systems and network management tools, etc. to provide electronic asset and configuration management data as required to the MSI.
(xviii) Comply with existing and established SMM processes.

### 9.8.5. Capacity Management

(a) Capacity Management assesses the current operations and future demands, pre-empting performance issues by taking the necessary actions before they occur.

(b) The Successful Respondent shall, at a minimum:

(i) Integrate Successful Respondent Capacity Management process and agreed data with the MSI's Capacity Management process and systems, including providing Successful Respondent Capacity data electronically to MSI's Capacity Management System in the agreed data format.
(ii) Communicate and coordinate the Capacity Management processes and policies within Successful Respondent's organization.
(iii) Actively cooperate in information exchange between and among the SCPs, MSI, DIR and DCS Customer to improve end-to-end Capacity Management.
(iv) Provide the means to automatically aggregate resource and system performance, system utilization, capacity limits for Successful Respondent Services.
(v) Provide the means to automatically calculate and forecast Successful Respondent Services capacity requirements through trending of collected data anticipating capacity needs.
(vi) In an automated manner, aggregate capacity information including current capacity and utilization, trends, issues and actions at the DCS Customer and Services level.
(vii) Initiate Incident Management, Problem Management or Request Management activities as needed to address Capacity Management issues and trends.

(viii) Action and track agreed capacity mitigations through associated Incidents, service requests, changes or projects using the MSI provided systems.
(ix) Participate and contribute to Capacity Management meetings.
(x) Incorporate appropriate capacity modeling to extrapolate forecasts of growth and other changes in response to projected DCS Customer business and operational needs.
(xi) Provide meaningful Capacity Planning input to the MSI-coordinated Capacity Plan.
(xii) Provide meaningful Capacity Planning input to the Technology Plan to develop requirements for long-range planning.
(xiii) Provide meaningful Capacity Planning input to the Refresh Plan to ensure Refresh and Technical Currency.

### 9.8.6. Refresh and Technical Currency

(a) The Successful Respondent will work with the MSI to ensure that technology refreshes of both hardware and software are done as scheduled and technical currency is maintained in the Services. An annual Technology Refresh Plan is required as a Critical Deliverable, as defined in **Attachment 1.1 Deliverables.**

(b) Successful Respondent's responsibilities include:

(i) Work with TSS, DCS SCPs, and DCS Customers to maintain application currency and ensure the developed application software will align with the DCS standard hardware and software platforms as described in the DCS Standard Configurations.
(ii) Upgrade and replace Equipment and Software (Refresh) as required in the Financial Responsibility Matrix throughout the Term, for purposes that include meeting DIR's and DCS Customers' business requirements; preventing technological obsolescence or failure; and accommodating volume changes, the ability to increase efficiency, the ability to lower costs, and/or the need to maintain the required Third-Party Vendor support.
(iii) Cooperate and coordinate on-going Refresh activities with the full Refresh Program at the direction of the MSI and in alignment with DCS Customer application upgrade activity.
(iv) Deploy Equipment and Software associated with any Refresh in accordance with the standards of DIR's technical architecture and the Technology Plan.
(v) Accommodate the timeframes and other requirements associated with Refresh, as well as the financial responsibility for the underlying assets, as provided in the Financial Responsibility Matrix.
(vi) DIR reserves the right to modify the Refresh timeframes and requirements during the Term based on its business requirements, subject to the Change Control procedures.
(vii) Cooperate, report, and support the management of Refresh Responsibilities by the MSI.
(viii) Where the Successful Respondent is financially responsible for Equipment and Software used in conjunction with the Services, as listed in the Financial Responsibility Matrix, Successful Respondent's responsibilities include:

A. Refresh the assets during the Term, including responsibility for the assets, the implementation, and ongoing support.
B. At a minimum and/or in the absence of a defined Refresh timeframe, maintain technical currency in accordance with Industry Standards.

(ix) Where DIR, SCPs, or and DCS Customers are financially responsible for Equipment and Software used in conjunction with the Services, the Successful Respondent will implement and support the new assets provided by DIR.

(x) Regardless of the ownership of underlying assets, Successful Respondent responsibilities include:

A. Provide personnel who are adequately trained in the use of the Equipment or Software to be deployed as part of the Refresh and provide such training prior to the Refresh.
B. Provide minimal disruption to DIR's and Customers' business operations associated with technology Refresh.

(xi) Use best practices and effective automation tools during Refresh deployment.

(xii) Perform all Changes to Equipment and Software in accordance with Change Management procedures.

### 9.8.7. Refresh Planning

The Successful Respondent will work with the MSI to ensure refresh planning is consistently done and in compliance with processes outlined in the Service Management Manual. Successful Respondent's responsibilities include:

(i) Develop a continual plan for Refresh, including:

(ii) Within one-hundred and twenty (120) days prior to, and no less than 10 business days ahead of DIR's annual planning process meetings, review the asset inventory and produce a report that lists the assets that are due to be refreshed in the upcoming plan year, and provide such report to DIR's annual planning process.

(iii) Cooperate and participate in the planning activities led by the MSI.

(iv) Successful Respondent and DIR will consider the usability of the assets and review alternatives to replace, re-lease, consolidate, or retain the assets. Based on the results of this review, Successful Respondent will deliver the initial recommendations regarding such assets to DIR within thirty (30) days after the review.

(v) For Successful Respondent-owned assets, Successful Respondent and DIR will mutually determine whether Successful Respondent will replace an asset and the appropriate replacement date.

(vi) If Software Changes are required due to replacement of assets, Successful Respondent, in consultation with the DIR, will review alternatives for making changes to such Software.

(vii) Such replacement of the assets and Software will be at Successful Respondent's expense if the replacement is required to facilitate achievement of the agreed upon Service Levels or because the asset is obsolete (i.e. replacement parts cannot be acquired, or the asset has become unserviceable).

(viii) For DIR and Customer owned and leased assets, based on the planning process outcome and direction established by DIR, Successful Respondent will provide a proposal for refresh of those assets (replacement at DIR's expense) to DIR.
(ix) Adhere to DIR's approved plan, and execute that plan utilizing established procurement processes, to initiate refresh and retirement activities.
(x) Provide monthly reports 180 days prior to lease expiration date showing assets to be refreshed with latest data.
(xi) Notify DIR monthly of all open agreements related to assets that are retired or will retire within 180 days of the report date.
(xii) Track and report on the completion progress of asset Refresh.
(xiii) Actively support TSS in workload assessment as part of refresh and annual technology planning.
(xiv) Update and archive asset records after retirement.

### 9.8.8. Request Management and Fulfillment Requirements

Successful Respondent shall be responsible for the fulfillment of Service Requests in compliance with processes in the SMM.

#### 9.8.8.1. Request Management Processes

The Successful Respondent shall, at a minimum:

(i) Actively participate with the MSI to develop and document processes.
(ii) Actively cooperate with the MSI in implementing and maintaining Request Management and Fulfillment processes that are flexible and facilitate effective communication and coordination across all functional areas.
(iii) Actively cooperate in information exchange between and among the Successful Respondent, the MSI, other SCP(s), DIR, and DCS Customer to improve end-to-end Request Management.
(iv) Integrate the Successful Respondent's Request Management process with the MSI's Request Management process and systems, where the processes interact.
(v) Facilitate the automation or mechanization of Service Requests between Successful Respondent and other SCP(s) systems.
(vi) Facilitate the transparency of Request Management through appropriate processes to provide a complete audit trail for the MSI to meet DIR and DCS Customer legislative and policy requirements.
(vii) Communicate and coordinate the Request Management processes and policies within Successful Respondent's organization.
(viii) Provide effective and agreed upon mechanisms for properly complying with the Request Management Policies.
(ix) Actively participate in developing and establishing Request for Solution processes and appropriate mechanisms for rapid proposal development that provides a level of accuracy for budgetary information without requiring a full solution.
(x) Actively work with the MSI in establishing processes and workflow for the proper routing of Service Requests.

#### 9.8.8.2. Service Request Operations

(a) Actively work with the MSI as appropriate to ensure the proper exercise of Request Management activities across all functions and organizations that provide Services to DCS Customers.

(b) Actively participate in Service Request tracking efforts and provide and maintain regular communications between all parties and Authorized Users through Request fulfillment.

(c) Manage the effective execution of Request Management for Successful Respondent to achieve its primary purpose to fulfill service requests within the agreed Service Levels and SMM and promote DCS Customer and Authorized User satisfaction.

(d) Work with the MSI to ensure that detailed audit trail information is recorded of all activity that creates, changes, or deletes data and user access to systems that contain DIR and DCS Customer data.

(e) Engage in effective Request Management governance process to enable the MSI in ensuring the following:

- (i) Clearly define and document the type of Service Requests that will be handled within the Request Management process so that all parties are clear on the scope of Service Requests and the Request Management process.
- (ii) Establish and continually maintain definitions of all Services, including: descriptions, Services that will be standardized, Services that require custom solutions, and Services that can be requested through each medium (e.g., Service Desk, Portal, Service Catalog, Request for Service).
- (iii) Establish and continually maintain Authorized User lists on who is authorized to make Service Requests and type of requests they are entitled to make.
- (iv) Communicate to DCS Customers the definition of Services, the Request Management processes, and changes thereto.
- (v) Participate in regular training for Authorized Users on Request Management processes, Service definitions, and request mediums.
- (vi) Perform regular collection of feedback from Authorized Users on the effectiveness of Request Management and engage in activities to improve process and service.

(f) Enable multiple mediums for accepting Service Requests, including the Service Desk, Portal, and Service Catalog.

(g) Enable the use of online self-service to allow Authorized Users to enter Service Requests from a pre-defined list of options.

(h) Enable the provision for real-time visibility of data records associated with Service Requests.

(i) Update required information on Service Requests within negotiated timeframes to provide an up-to-date accurate view of Service Requests.

(j) Ensure proper approval, including financial authority, or the Service Request through automated means (where practical) prior to Service Request fulfillment.

(k) Provide and maintain regular communications between all parties and Authorized Users as required until Service Request completion and document the communications in compliance with the Request Management processes.

(l) The communications frequency shall be determined by the severity of the request and in compliance with the SMM.

(m) Keep DCS Customer and MSI informed of any issues with the completion of Service Requests and status changes throughout the Service Request lifecycle and in accordance with the SMM.

(n) Provide anticipated completion times for active Service Requests and update notification systems as required in the SMM to keep DCS Customers and Authorized Users informed in compliance with established Service Levels.

(o) Work with the MSI to ensure consistent ownership of the Service Request from recording to completion.

(p) Close Service Requests, in compliance with the SMM, after receiving confirmation from the requesting Authorized User or Successful Respondent support personnel that the Service Request has been completed.

(q) Track the progress of fulfillment efforts and the status of all Service Requests, including:

- (i) Review the proposed fulfillment time for each Service Request with the appropriate party and update the status accordingly.
- (ii) Provide regular updates on the status of all Service Requests within designated timeframes.
- (iii) Coordinate Service Request tracking efforts and provide and maintain regular communications, per the SMM, between all parties and Authorized Users until Service Request completion.
- (iv) Keep the DCS Customer and Authorized User informed of changes in Service Request status throughout the Service Request lifecycle in compliance with the SMM.
- (v) Keep DCS Customer informed of anticipated Service Request completion times for active Service Requests.
- (vi) When a Service Request cannot be completed in the committed timeframe, provide a revised completion time or request a meeting with the Authorized User to determine a new timeframe.
- (vii) Track all Service Request completion against the original committed timeframe, regardless of any revisions.

(r) Utilize the Request Management System provided by the MSI for all Request Management and Fulfillment activities.

(s) Provide for timely receipt and processing of all requests within designated timeframes from the Request Management System.

(t) Utilize and update the Request Management System with all relevant information relating to a Service Request.

#### 9.8.8.3. Request for Solution (RFS)

Requests for Solution (RFS) are those types of DCS Customer requests where requirements are captured in the MSI request management system and SCP's develop solutions and cost estimates for DCS Customer review and approval. These solutions typically assume the SCP builds and implements the solution. For DCS Customer Requests, which require the Successful Respondent to propose a solution, the Successful Respondent's shall, at a minimum:

(i) Work with TSS and the MSI in developing and establishing RFS processes and appropriate mechanisms for the fulfillment of complex requests requiring design, price, solution, and proposals; including appropriate communications to adequately set expectations and promote good customer service.

(ii) Work with TSS and the MSI in developing and establishing RFS processes and appropriate mechanisms to ensure rapid proposal development that provides a level of accuracy for budgetary information without requiring a full solution (e.g., rough order magnitude pricing and high-level architecture).

(iii) For all RFS delivered by the Successful Respondent only and that require no other SCP support:

A. Review RFS to validate for completeness.
B. Coordinate and lead meetings as required to review request, gather requirements, solution and develop the proposal.
C. Coordinate the attendance of all necessary subject matter experts in solution and requirement gathering sessions.
D. Provide a timeframe for delivering the solution proposal, including cost estimates, once requirements are complete.
E. Develop the solution which may include the technical solution, effort, acceptance criteria, solution design document, and pricing.
F. Ensure all solutions to requests conform to the DIR-approved architecture, standards, and pricing.
G. Ensure all solutions to requests conform the security policies, procedures, and guidelines of DIR.
H. Ensure all solutions to requests conform within the bounds and guidelines of DIR Shared Services technical guidelines.
I. Ensure all solutions to requests conform within the bounds and guidelines of the Contract.
J. Coordinate and facilitate solution reviews across the Successful Respondent as required to review and gain approval for the solution and pricing.
K. Track all Project Change Requests in accordance with established procedures.
L. Provide a single proposal to requesting DCS Customer.
M. Iterate and adjust the solution and cost estimating template as required to adhere to the requesting DCS Customer's feedback and requirements.
N. Document DCS Customer approvals in accordance with established processes as per the SMM.
O. Gather and validate that the proposal acceptance comes from an appropriately authorized user.

P. Provide status to DIR and DCS Customers status of all outstanding requests such that DCS Customers can emphasize their organizational priorities.

Q. Initiate Project Management as appropriate upon proposal acceptance by DCS Customer.

(iv) For an RFS where the Successful Respondent is one of many SCPs, lead and manage the Successful Respondent's solution development and project delivery using the approved MSI Shared Services Systems and processes and work with TSS, the MSI, and the other SCPs as required to develop a coordinated DCS Customer solution, including executing the RFS processes and appropriate mechanisms for the fulfillment of Successful Respondent assigned requests requiring a solution (e.g., requirements, design, solution, price, proposal) and project delivery (e.g., plan, build, testing, cutover).

A. Solution the Successful Respondent's portion of the RFS, including:

1. Participate in meetings as required to review requests, gather requirements, solution and develop proposals with other SCPs, DIR, DCS Customers, and other Third-Party Vendors.
2. Coordinate the attendance of all necessary Successful Respondent subject matter experts in solution and requirement gathering sessions.
3. Adhere to the TSS provided timeframe for delivering a solution proposal, including cost estimates, once requirements are complete.
4. Ensure all requests are solutioned within the DIR-approved architecture and standards and pricing.
5. Ensure all requests are solutioned within the security policies, procedures, and guidelines of DIR.
6. Ensure all requests are solutioned within the bounds and guidelines of DIR Shared Services technical guidelines.
7. Ensure all solutions to requests conform within the bounds and guidelines of the Contract.
8. Participate in solution reviews across the Successful Respondent and all affected SCPs as required to review and gain approval for the solution and pricing.
9. Contribute to the solution development, cost-estimation, project plan, status, issues and risks in the systems and in compliance with the processes in the DIR-approved SMM.
10. Tracking of all Project Change Requests in accordance with established procedures.
11. Work with TSS in their development of a single proposal to the requesting DCS Customer.
12. Iterate and adjusts solution and cost estimation as required to adhere to the requesting DCS Customer's feedback and requirements.
13. Initiate Project Management activities, according to the SMM, upon proposal acceptance by DCS Customer.

B. Assist TSS resources in development in of high-level assessments, conceptual designs, and ROM proposal as requested.

### 9.8.9. Asset Inventory and Management

(a) Asset Inventory and Management System provides an inventory of the IT infrastructure managed by the Successful Respondent. The MSI consolidates information from multiple Successful Respondent Asset Inventory and Management Databases that contain details of Equipment, Software, and similar IT service items (collectively referred to as CIs) used in the provision, support, and management of IT services. Automated collection of asset and configuration data is a key component of the Service allowing for real-time reporting and management of DCS components.

(b) Successful Respondent responsibilities include:

(i) Actively participate with the MSI to develop and document Asset Inventory and Management processes, as approved by DIR, that document the objectives, scope, and principles that ensure the success of the Asset Inventory and Management processes.

(ii) Integrate Successful Respondent Asset Inventory and Management process with the MSI's Asset Inventory and Management process and systems, including providing Successful Respondent asset data electronically to MSI's Asset Inventory and Management System (AIMS) in the agreed data format.

(iii) Provide automation for all integration with the MSI's Asset Inventory and Management process and systems inclusive of auto-discovery functions to ensure real-time reporting of DCS infrastructure components.

(iv) Communicate and coordinate the Asset Inventory and Management processes and policies within Successful Respondent's organization.

(v) Actively cooperate in information exchange between and among the SCPs, MSI, DIR and DCS Customer to improve end-to-end Asset Inventory and Management.

(vi) Work with the MSI to provide a complete Asset Inventory and Management audit trail to meet DIR and DCS Customer legislative and policy requirements.

(vii) Conform operations to policies and procedures that set the objectives, scope, and principles that ensure the success of the Asset Inventory and Management process.

(viii) Work with the MSI in establishing categorization and classification structures to ensure the proper documentation and maintenance of CIs.

(ix) Use the Asset Inventory and Management process to identify, control, maintain, and verify the CIs approved by the MSI as comprising the Equipment, Software, and Applications to provide the Services.

(x) Record the CI information for Equipment, Applications, Software and Services.

(xi) Verify that all CIs for the Equipment, Applications, Software, and Services are incorporated into the AIMS.

(xii) Utilize the AIMS provided by the MSI as the single source of information regarding all CIs within Successful Respondent scope.

(xiii) Ensure that all CI data related to the Services resides in the AIMS.

(xiv) Integrate the Successful Respondent's other systems, including all appropriate and required licenses and/or interfaces with the MSI's AIMS.

(xv) Where Successful Respondent has an internal asset inventory system or database, integrate that system or database with the MSI AIMS as required.

(xvi) Provide customization as required to enable the Asset Inventory and Management processes as defined in the SMM.

(xvii) Automate processes, discovery tools, inventory and validation tools, enterprise systems and network management tools, etc. to provide electronic Asset Inventory and Management data as required to the MSI.

(xviii) Comply with existing and established SMM processes.

### 9.8.10. IT Service Desk Requirements

(a) Successful Respondent shall be responsible for responding to incidents or requests DCS Customers log with the MSI's Service Desk, in compliance with policies and procedures set forth in the SMM and managed by the MSI.

(b) The MSI's Service Desk shall be the single point of contact for BAE regarding Incidents, which include events that cause or may cause an interruption or reduction of service, as well as for requests for information and requests for services relating to all of DIR's and DCS Customers' IT Services.

(c) The Successful Respondent shall, at a minimum:

(i) Actively participate with the MSI to develop and document processes.

(ii) Integrate Successful Respondent's Service processes with the Service Desk processes of the MSI, DCS Customer, and authorized Third Party Vendor(s), where the processes interact.

(iii) Actively work with the MSI to assure the proper application of Service Desk across all functions and organizations that provide services to DCS Customers.

(iv) Communicate and coordinate the Service Desk processes and policies within Successful Respondent's own organization and DCS Customers.

(v) Actively participate in defining Service Desk policies and procedures, as approved by DIR, which set the objectives, scope, and principles that ensure the success of the Incident Management processes.

(vi) Provide effective and agreed upon mechanisms for properly complying with the Service Desk policies.

(vii) Manage all Incidents, Service Requests, etc., from Authorized Users relating to Services, including the following:

A. Assigning categorization and prioritization codes.

B. Communicating with users, keeping them informed of progress, notifying them of impending actions, obtaining appropriate agreement, and in all ways engaging and communicating with them about Successful Respondent activities.

C. Closing all resolved Incidents, Service Requests, and other calls.

(viii) Develop and document processes regarding interfaces, interaction, and responsibilities between Level 1 Support personnel, Level 2 Support personnel, and any other internal or external persons or entities that may either submit an Incident or receive an Incident.

(ix) Utilize the Incident Management System provided by the MSI and integrate with the MSI Service Desk, including the use of tools, technology, processes, and procedures.

(x) Analyze Incident trends and recommend and implement actions, with DIR and DCS Customer(s) approval, to reduce Incidents.

(xi) Provide on-line FAQs and help documentation for common problems.
(xii) Provide the MSI with information necessary to keep Authorized Users regularly updated with alerts advising of any new or changed information.

### 9.8.11. Information Security Management Requirements

Successful Respondent's delivery of Information Security Management shall be an integral part of the Services and shall assess all security risks associated with the delivery of Services are appropriately identified, evaluated, assessed and appropriate controls are implemented and maintained.

#### 9.8.11.1. Information Security Management General Requirements

The Successful Respondent shall, at a minimum:

(i) Work with the MSI in support of the overall Cybersecurity risk management program.
(ii) Work with the MSI to develop and maintain security procedures and Service Responsibility Matrices, physical and logical access strategies, and standards.
(iii) Adhere to the Information Security Management processes as defined in the SMM.
(iv) Work with the MSI to integrate Successful Respondent's security program with DIR's governance risk and compliance program, including at a minimum Incident recording, CMDB, security exception, security plan submission, risk assessment and in integrating Successful Respondent's Security tools directly with the MSI as required to enable these capabilities.
(v) Implement security capabilities as required to achieve compliance with security laws, rules and regulations.
(vi) Participate in security evaluations, as directed by DIR, which include conducting internal audits, supporting external audits, conducting self-assessments, and evaluating security Incidents.
(vii) Participate in all DIR authorized assessments, develop action plans and resolve deficiencies, vulnerabilities, concerns and recommendations identified within six (6) months of the conclusion of the assessment or at such time as otherwise mutually agreed upon.
(viii) Meet all Security-related deliverables and Performance Analytics which are to be agreed to by DIR and Successful Respondent.
(ix) As requested, attend and contribute to Security Management and Risk Management meetings.
(x) Resolve agreed actions and activities resulting from Security Management meetings.
(xi) Work with the MSI and contribute to the creation and maintenance of a Security Plan across the Successful Respondent's Services.
(xii) Execute Successful Respondent's Security Plan which is agreed to by DIR and coordinated by the MSI.
(xiii) Ensure that certificates for Successful Respondent's staff are kept current and report the status to the MSI on a quarterly basis.
(xiv) Provide for vulnerability scans for all Successful Respondent network assets, which should include scans for all network addresses at least once per year directly to the

DIR Governance, Risk and Compliance (GRC) tool (Currently SPECTRIM) and inform the MSI.

(xv) Provide a forward-looking schedule for the planned Successful Respondent Security testing, assessments and analysis.

(xvi) In coordination with the MSI, participate in the evaluation of new technologies/capabilities for improving security and perform activities and/or solutions to address shortfalls in Security.

(xvii) Where investment decisions are required, work with the MSI in providing options with associated costs and benefits for DIR review and approval.

(xviii) In coordination with the MSI, and as related to the Successful Respondent's Services, evaluate details of the Security requirements for new IT services, including options for meeting these requirements and any associated costs.

(xix) Work with the MSI and execute processes according to the governance-approved Master Security Baseline Configuration (MSBC).

(xx) Execute quarterly MSBC Health Checks and run scans quarterly that will feed baseline information to the MSI for the MSI to determine the health check of the systems.

#### 9.8.11.2. Successful Respondent Staff

The Successful Respondent shall, at a minimum:

(i) Limit access to and use of data to authorized Successful Respondent personnel only.

(ii) Successful Respondent personnel must have received security clearance and successfully complete a background and criminal history investigation prior to performing contract functions or accessing DIR, DCS Customer Facilities, Systems, Networks or Data.

A. Criminal history background checks are to be conducted per Texas Government Code (TGC) Subchapter F, Section 411.1404 and will be in compliance with the then-current versions of the FBI CJIS Security Policy and the FBI CJIS Security Addendum. In addition, an annual background check re-verification is required. DIR must be notified of the compliance with the initial criminal history background check and the annual re-verification.

B. Background and criminal history background checks will be performed by the Texas Department of Public Safety and the Texas Department of Criminal Justice. Other DCS Customers may require additional levels of compliance as per agency regulations and policies.

C. Successful Respondent is responsible for any costs associated with the criminal history background check process.

D. Successful Respondent will establish a process that facilitates the timely submission and resolution of the criminal history background checks, including but not limited to using digital methods to submit necessary criminal history background check requirements.

(iii) Define processes and procedures for automated tracking of Clearances for all Successful Respondent personnel and Third-Party Vendors utilizing the Security Clearance Management System provided by the MSI.

#### 9.8.11.3. Security Regulations

The Successful Respondent shall:

(i) Adhere to the then-current safety and security policies, rules, procedures and regulations established by the State and DIR, and each DCS Customer with respect to such DCS Customer's data and facilities.

(ii) Adhere to DIR and DCS Customer's then-current "Security Rules," as published in Chapter 202, Information Security Standards of the Texas Administrative Code.

(iii) Comply with all security incident notification and response procedures as specified in the Service Management Manual.

(iv) Comply with the policies defined by the FBI Criminal Justice Information Services (CJIS) requirements.

(v) The Successful Respondent shall perform the Services in compliance with all federal and state laws and industry standards as they may be updated from time-to-time, including but not limited to the following:

A. Texas Administrative Code (TAC) 1 Chapter 202. TAC 202 provides the State of Texas security standards policies applicable to all Texas state agencies.
B. HIPAA – Health Insurance Portability and Accountability Act Privacy and Security Rules
C. HITECH – Health Information Technology for Economic and Clinical Health Act
D. FIPS 140-2 Federal Information Processing Standards Publication, Security Requirements for Cryptographic Modules
E. FISMA – Federal Information Security Management Act
F. FERPA – Family Educational Rights and Privacy Act
G. IRS Pub 1075 – Tax Information Security Guidelines for Federal, State and Local Agencies
H. PCI – Payment Card Industry Security Standards
I. ISO/IEC 27001:2005 - Information technology – Security techniques – Information security management
J. ISO/IEC 27002 – code of practice for information security management
K. NIST 800 – National Institute of Standards and Technology standards and related publications
L. CJIS Security Policy - FBI Criminal Justice Information System Security Policy and CJIS Security Addendum

(vi) DIR and DCS Customers comply with National Institute of Standards and Technology (NIST) Federal standards and related NIST 800 series Special Publications (SP) and Federal Information Processing Standards (FIPS) standards. Where there is a conflict between NIST, FIPS and 1 TAC Chapter 202 rules and security controls, the 1 TAC Chapter 202 takes precedence.

#### 9.8.11.4. Security Incident Management

The Successful Respondent shall, at a minimum:

(i) Work with the MSI and contribute to the creation of a Security Incident Management Plan across the Successful Respondent's Services.
(ii) Provide plans and exceptions for all Security Incident Management plans including Security Incident severity matrix, notification rosters, communications plans, and procedures for managing Security Incidents.
(iii) Implement the Successful Respondent's portion of the Security Incident Management Plan in concert with participation from the MSI and required SCPs and DCS Customer personnel.
(iv) Coordinate Security Incident Management procedures with Major Incident Management procedures.
(v) Adhere to the Security Incident handling and notification processes that follow current NIST guidelines and is defined in the SMM.
(vi) As required, implement and maintain monitoring and alerting services that integrate into the MSI Incident Management System and Security Operations SIEM for automated alert notification.
(vii) Promptly investigate, document, and report Security Incidents in accordance with 1 TAC Chapter 202 and the SMMs.
(viii) According to the defined processes, promptly communicate and escalate security Incidents to the MSI, Security provider, DCS Customer, and DIR.
(ix) Conduct Root Cause Analysis and if necessary, develop and implement formal corrective actions or remediation plans once approved by DIR and the appropriate DCS Customer. Evaluate the analysis and proposed corrective actions to ensure future risks are adequately mitigated.
(x) Provide Incident investigation and initiate corrective actions to minimize and prevent security breaches.

#### 9.8.11.5. Physical Security Administration

The Successful Respondent's shall, at a minimum:

(i) Communicate the physical and logical security management processes and procedures to Successful Respondent's staff.
(ii) Comply with Successful Respondent physical and logical security responsibilities.
(iii) Inform MSI and DCS Customer immediately if Successful Respondent becomes aware of any vulnerability or weakness in the Services and recommend a solution or mitigation.
(iv) Provide near real-time information, to MSI and DCS Customers to identify those physical access rights that should be removed from MSI and DCS Customer Facilities and where, within the Successful Respondent's scope of responsibilities, initiate the access rights revocation request.

#### 9.8.11.6. DIR and DCS Customer Sites

(a) Where Successful Respondent uses or visits locations and facilities at DIR and DCS Customer Sites, Successful Respondent shall be responsible for the provision of Services related to DCS Customer's

security requirements, set in place by DCS Customer to govern the security of the DCS Customer Environment.

(b) Successful Respondent shall, at a minimum:

(i) Ensure compliance with all DIR and DCS Customer security policies, standards and procedures, and all applicable laws and regulations, as they may be revised or updated.
(ii) Comply with DIR and DCS Customers' policies, including security, data and records management, and electronic records and data archiving.
(iii) Implement the security-related Services required to protect the confidentiality, integrity, and authenticity of the information stored in or transmitted to or from the DCS Customer environment, in accordance with DCS Customer's security requirements.
(iv) Comply with DIR's, DCS Customers', and SCPs' Physical Security Administration processes, where the processes interact.
(v) Assist in the development of action plans following any Security Incidents within the DCS Customer environment and implement new controls approved by DCS Customer and in the timeline defined by DCS Customer.
(vi) Maintain DIR Data in accordance with DCS Customer's security policies.
(vii) Establish and maintain safeguards against the unauthorized access, destruction, loss, or alteration of DIR Data in the possession of Successful Respondent in accordance with DCS Customer's security policies.
(viii) Participate in Service Delivery to review any Changes to the Equipment, Software, and networks that potentially have security or operational ramifications and modify the Change to remove or reduce the security or operational ramifications.

#### 9.8.11.7. Other Locations

Where Successful Respondent uses other locations and facilities to provision Services to DIR or DCS Customers, Successful Respondent's responsibilities shall include the following:

(i) Provide security processes, facilities, Equipment, and Software that meet or exceed DIR's security policies, standards, and procedures. Such processes and physical attributes will be at a minimum consistent with similar security provisions maintained by large, well-managed sourcing services companies.
(ii) Upon request, provide DIR, its representative(s), and/or regulatory DCS Customers access to all facilities and assets used in providing the Services for audits, investigations, and compliance reviews.
(iii) Perform all physical security functions (e.g., identification badge controls and alarm responses) at facilities under Successful Respondent's control.

#### 9.8.11.8. Security Assessments

(a) The following applies to Successful Respondent security assessments:

(i) DIR may initiate and conduct assessments of Successful Respondent's security program. Such assessments will evaluate Successful Respondent's abilities and capabilities in maintaining and enhancing security and safety practices and procedures, and may involve monitoring and testing security programs, conducting risk assessments and performing security design reviews.

(ii) DIR, DCS Customers, Texas State Auditor's Office, and other entities authorized by DIR may conduct security reviews, assessments, forensic analysis and/or audits (e.g., SSAE 18, State Audit Office, IRS audits) where service is being provided by the Successful Respondent. These assessments may include (but are not limited to) physical security, logical security, policies and procedures, network analysis, vulnerability scans and Controlled Penetration Tests.

(b) The following applies to Assessments in general:

(i) DIR may conduct security assessments, including conducting monitoring and testing security programs (e.g., Controlled Penetration Tests), conducting risk assessments and performing Security Design Reviews, (the "Assessment(s)") of all or any portion of the Services in order to evaluate such Security Program and determine whether the Security Program meets or exceeds the Standard of Due Care.

(ii) Assessments of the Security Program may be conducted by DIR or, at DIR's sole discretion, a third-party security assessment vendor (the "Security Assessment Company").

(iii) The Successful Respondent shall cooperate fully with DIR and/or the Security Assessment Company and provide access to any premises, equipment, personnel or documents and provide any assistance required by DIR and/or the Security Assessment Company to conduct the Assessment; however, DIR and the Security Assessment Company shall not have access to Successful Respondent proprietary information where it is not relevant to the Assessment, and shall further not have access to confidential or proprietary information of other customers of Successful Respondent than DCS Customers.

(iv) Under no circumstances will Successful Respondent attempt to persuade or control or otherwise influence the Security Assessment Company in the determination of its findings. The Assessment shall be conducted so as not to unreasonably disrupt Successful Respondent's operations under this Agreement.

(v) Within fifteen (15) days of an Assessment Notice Date, DIR and Successful Respondent will meet to jointly review the relevant Assessment report and if such report concludes that the Security Program does not meet or exceed the Standard of Due Care, then within thirty (30) days after the applicable Assessment Notice Date, the Successful Respondent and the MSI shall develop and present to DIR an action plan to promptly address and resolve any deficiencies, vulnerabilities, concerns and/or recommendations identified in such report, consistent with the Successful Respondent's obligations as set forth in the Agreement.

### 9.8.12. Software License Renewal Management

Successful Respondent has responsibility for:

(i) Working with the MSI in tracking, monitoring, and reporting the software renewal process to ensure compliance with software agreements and continued operation of Services. Successful Respondent's responsibilities shall include the following:
(ii) Comply with the Software License Renewal Management processes, as defined in the SMM.
(iii) Support Service Requests and Change Requests as appropriate for all renewals and update as needed to reflect the status of each renewal as per the timing and lifecycle process defined in the SMM (e.g., Software expiring in May should be logged as a CRQ in January, 120 days prior to the expiration date).
(iv) Successful Respondent will update the contract data in the approved Software License Renewal System, coordinate with the DCS Customer and MSI to obtain renewal approvals, execute the procurement tasks to renew the software license, install the renewed keys and software, update the Change Request and Contracts data, and log the renewed software keys in the Software License Renewal System as per the process defined in the SMM.
(v) In conjunction with the MSI, monitor Software License Renewal progress and SLA achievement.
(vi) Work with the MSI to ensure the requests and Change Requests are completed and closed upon renewal completion.

#### 9.8.12.1. Software License Compliance Management

The Successful Respondent will:

(i) Work with the MSI to determine the compliance position, based on automated monitoring and reporting of the software compliance management process to ensure compliance with agreements and reduce operating risk in the environment. Successful Respondent's responsibilities shall include the following:
(ii) For Successful Respondent provided and managed software, execute assigned Software License Compliance Management activities as defined in the SMM.
(iii) For DIR and DCS Customer-retained Software, track and maintain the applicable licensing and use information received from DCS Customers.
(iv) If applicable, utilize tools, such as an enterprise management system and remote monitoring agents, to assist in monitoring efforts, subject to DIR's approval of all such tools.
(v) Monitor the Equipment for the presence of any unauthorized or non-standard Software.
(vi) Define and check for particular Software signatures.
(vii) Check the presence and version of Software installed on a particular device and record in the MSI Asset Inventory and Management system.
(viii) Provide reporting of license information and compliance to the MSI, at least quarterly or as directed by DIR.
(ix) Store and track Software license agreements and associated license keys, including processes and procedures for renewals.
(x) Track license counts and associations within the CMDB.

(xi) Collect and maintain the Contract and Proof of Entitlement (POE) within the MSI-provided system.
(xii) Work with the MSI to collect and normalize software titles to standard names.
(xiii) Work with the MSI to review the Software License Compliance position and determine appropriate remediation.
(xiv) Take ownership of assigned actions through the Incident, Request, Change, and Project processes for any reported non-compliance of software purchased versus software installed.
(xv) Provide clarifications about information presented in the Compliance Report to eliminate discrepancies.
(xvi) Enable the use of Successful Respondent provided and managed Software to maintain strict compliance, including but not limited to:
A. Immediately notify and advise MSI of all Software license compliance issues associated with Services.
B. Enable the tracking, management and implementation of security certificates used to secure confidential sessions (e.g., SSL) for Internet and Intranet transactions and communications, including processes and procedures for renewals, as required by DIR, DCS Customers, or MSI.
(xvii) Work with the MSI to confirm the presence and version of Software installed on a particular device and that those attributes are recorded in the MSI Asset Inventory and Management system.
(xviii) Work with the MSI in reporting of license information and compliance to DIR.

#### 9.8.12.2. Software Patch Management

The Successful Respondent shall, at a minimum:

(i) Be responsible for patch deployment and control of the software and devices under its management.
(ii) Be responsible for participating in DCS Customer Change Management processes to deploy patches on a regular basis.
(iii) Participate in and follow the agreed upon patch rating process.
(iv) Deploy patches to servers and clients per DCS Customer's policies and ensure compliance as required. Use the DCS Customer-approved central deployment tool, as applicable and mutually agreed upon.
(v) Provide and apply patches to devices within the timeframe guidelines in accordance with DCS Customer's security policies.
(vi) Adhere to DCS Customer's security configuration management.
(vii) Communicate with and/or alert the DCS Customer IT Security team when patches are not installed within the designated timeframe.
(viii) Integrate and have the ability to export patch data associated will all DCS Customer devices.

### 9.8.13. IT Service Continuity Management Requirements

(a) Successful Respondent is responsible for maintaining an IT Service Continuity Management (ITSCM) plan for its own internal staff and systems to respond to an emergency and continue to provide Services to DIR and DCS Customers.

(b) The Successful Respondent shall, at a minimum:

(i) Develop, maintain, and test Disaster Recovery Plans (DRPs) and Technical Recovery Guides (TRGs) as defined in the SMM for the Systems, Software, and Equipment used by Successful Respondent to provide the Services, including those provided at the Consolidated Data Centers, DCS Customer Service Location, or other Successful Respondent Facilities.

(ii) The DRPs and TRGs should comply with all applicable Federal and State requirements.

(iii) In the event of a disaster, recover and support affected Systems, Software, and Equipment at the designated recovery location according to the agreed Recovery Time Objective (RTO) and Recovery Point Objective (RPO) in support of the Service Levels defined in this Exhibit.

(iv) Coordinate Successful Respondent's ITSCM plan with MSI ITSCM plans and DCS Customer Business Continuity Plan (BCPs) to ensure DCS Customers can resume regular business functions in the event of a Disaster or significant event affecting the Systems, Software, and Equipment used by Successful Respondent to provide the Services.

(v) In the event of a service disruption, coordinate all ITSCM efforts to ensure smooth and efficient resumption of Services.

#### 9.8.13.1. Crisis Management

The Successful Respondent will perform Crisis Management as necessary, depending on the type of business or geographic location where Services are being performed, in the event of hurricanes, tornados, riots, terrorist threats, etc. The Successful Respondent shall, at a minimum:

(i) Following MSI, DIR, and DCS Customer notification processes for any crisis event occurring in or relating to a Successful Respondent Facility, DIR Facility, or other facilities managed by Successful Respondent in connection with the Services.

(ii) Following statewide notification pyramid alert support as documented in the applicable business continuity plan.

(iii) Coordinate with MSI, DIR, and DCS Customers requirements for Services that are critical to designated DCS Customer emergency management responsibilities.

(iv) Coordinate with MSI, DIR, and DCS Customer regarding variances in Services as a result of Crisis Management in compliance with all SMM procedures.

### 9.8.14. Release Management

(a) The purpose of Release Management is to build, test and deliver specified Services that will accomplish the stakeholders' requirements and deliver the intended objectives.

(b) The Successful Respondent shall, at a minimum:

(i) Work with the MSI and other SCPs to develop and establish a Release and distribution process so that each change to Service Provided Services is controlled, tested, traceable, authorized, and implemented in a structured manner.
(ii) Conform Successful Respondent operations to the agreed Release policies, processes and procedures as defined in the SMM.
(iii) Execute releases according to the approved Release Management methodology as defined in the SMM.
(iv) Use the MSI provided Release Management System as the single source of Release Management and information regarding all Successful Respondent Releases.

### 9.8.15. Project Management

(a) Project Management provides a way to execute and manage projects with the goal of delivering projects from request through completion, meeting DCS Customer requirements in terms of timing, quality, and cost.

(b) The Successful Respondent shall, at a minimum:

(i) Provide technical project management and be responsible for executing and managing projects related to the Successful Respondent's Services.
(ii) Conform Successful Respondent operations to MSI-defined policies and procedures as documented in the SMM to ensure the success of the Project Management process.
(iii) Use the MSI provided Project and Program Management (PPM) system as the single source of project management and information regarding all projects and programs.
(iv) Ensure that all Successful Respondent Project Management data resides in the PPM system.
(v) Execute projects according to the approved Program Management and Project Management methodology as defined in the SMM.

(c) Projects that meet the criteria for "major information resources project", as defined by Texas Government Code 2054.003 (10), are subjected to state Quality Assurance Team (QAT) oversight requiring the Successful Respondent to support the following:

(i) Adhere to the requirements and guidelines as outlined in the Project Delivery Framework located here: http://dir.texas.gov/View-Resources/Pages/Content.aspx?id=16.
(ii) Provide project deliverables as required for the QAT to review and provide proactive monitoring of project outcomes.
(iii) Develop and execute corrective action plans for projects with QAT identified project risks.
(iv) Provide status reports to TSS, MSI and DIR as required to report to QAT stakeholders (state leadership, DIR leadership, DIR, TSS and MSI project teams).
(v) Escalate significant issues to TSS, MSI and DIR and advise on alternative methods for correction.

## 9.9. Business Management

### 9.9.1. Operational Intelligence

(a) Successful Respondent shall provide the data and/or reports to the MSI via automated API integration for report creation and posting via the MSI-managed Operational Intelligence System and Portal as specified in **Appendix A Reports** and Service Level reports as defined in Service Levels.

(b) The Successful Respondent shall, at a minimum:

(i) For core Services, provide online reporting capability with near real-time data for use by DCS Customers in the generation of sophisticated, custom reports.

(ii) As agreed with DIR, coordinate with the MSI to provide single sign-on access to Successful Respondent's reports through the MSI Portal.

(iii) As appropriate, provide near real-time operational data feeds to the MSI-managed Operational Intelligence System.

(iv) Provide on-time, monthly service-level performance data for each Service Level requirement, to the MSI-managed Service Level Management System.

(v) Provide mutually agreed upon reports and data to the MSI to enable invoice reconciliation.

(vi) Coordinate with the MSI and provide data to enable the creation of integrated performance dashboards. Dashboard data should provide:

A. Near real-time health dashboards for any Systems managed by Successful Respondent highlighting status of health metrics as defined by DCS Customer.

B. Report monthly, quarterly, and annually in the Security Dashboard on the deployment of Tools and procedures to the DCS Customer Environment.

(vii) The Successful Respondent shall be responsible for using DIR's security governance, risk and compliance system to provide information relevant to the service offering, including but not limited to risk assessments, Incident reporting, and security plan development.

(viii) As required, collaborate with other DCS SCPs, to include sharing reports and information via the MSI Portal or other mutually agreed upon mechanism as appropriate to ensure effective Service delivery.

(ix) Enable integration of applicable security Service solutions, in which data from multiple sources (e.g., scan results, multiple IDS platforms/IPS devices, and MDS devices) are incorporated and integrated into the Service.

(x) Provide ad hoc and summary Security Incident Reports to DIR OCISO using security systems and data generated in accordance with the format and content of the then current version of 1 TAC Chapter 202.

### 9.9.2. Service Level Management

(a) Service Level Management includes the activities associated with managing and reporting attainment of Service Level performance, deliverable commitments, and customer satisfaction.

(b) The Successful Respondent shall, at a minimum:

(i) Provide accurate and timely SLA data to the MSI as defined in Article 6 Performance Model – Service Level Agreements, and the SMM to the MSI-managed Service Level Management System as agreed with the MSI (e.g., format, timing, delivery mechanism).

(ii) When SLAs fail to meet minimum, or expected service level targets, implement Service Level Improvement Plans (SLIP), as described in the SMM.

(iii) Analyze DCS Customer Scorecard feedback to understand DCS Customer issues and develop and execute issue resolutions.

(iv) Collate information provided to Successful Respondent from End Users (e.g., captured in Service Desk surveys, feedback through emails) regarding suggested improvements to the Services.

(v) Develop an action plan to address suggested improvements to the Services identified by Successful Respondent and DCS Customer, including the following:

A. Provide the action plan to DCS Customer for review.

B. Implement DCS Customer-approved action plans.

C. Report in the Dashboard on progress and improvements made on approved action plans.

(vi) Summarize and report on plans and activities that affect the overall Services to MSI and DIR governance boards.

### 9.9.3. IT Financial Management

Successful Respondent must provide automated IT Financial Management Services via API. The Successful Respondent shall, at a minimum:

(i) Actively work with the MSI to develop and document IT Financial Management processes.

(ii) Actively cooperate in information exchange between and among the MSI, DIR, and DCS Customer to improve end-to-end IT Financial Management.

(iii) Facilitate the transparency of IT Financial Management through appropriate processes to provide a complete audit trail for the MSI to meet legislative and policy requirements.

(iv) Integrate Successful Respondent IT Financial Management process and system with the MSI's IT Financial Management process and system, where the processes interact, and as agreed to with DIR and the MSI.

(v) Actively work with the MSI to assure the proper application of IT Financial Management across all functions and organizations that provide services to DCS Customers.

(vi) Communicate and coordinate the IT Financial Management processes and policies within Successful Respondent's own organization.

(vii) Utilize the IT Financial System provided by the MSI such that it serves as the single source of information regarding all IT Financial Information for Services within Successful Respondent scope.

(viii) Integrate Successful Respondents' systems and chargeback data with the MSI IT Financial System, including providing all appropriate and required licenses and/or interfaces.

(ix) Provide sufficient data and detail to support DIR, DCS Customers, State and Federal funding accounting, grant, and audit requirements.

(x) Collect, aggregate, and provide billing, service provisioning, and service metric information to the MSI as required.

(xi) Identify unique DCS Customer account identifiers to identify Applications, Application Instances, and other service information as required.

(xii) Provide the MSI with monthly invoice data required for the MSI to render the Successful Respondent statement of Services.

(xiii) Support all charges with detailed invoice data as required, and supporting utilization data at the DCS Customer, Resource Unit, Charge Category (e.g., Programs, Divisions, Organization Units) as required by the MSI.

(xiv) Actively participate in developing and maintaining the processes for the resolution of invoice disputes within designated timeframes.

(xv) Provide effective and agreed mechanisms for crediting DCS Customers as appropriate.

(xvi) Effectively execute the processes to record, track, and manage incidents of invoice disputes.

(xvii) Research and review invoice disputes for completeness and ensuring data accuracy, and, when necessary, request clarifying data from DCS Customer.

(xviii) Initiate additional treatment of invoice disputes to facilitate resolution within designated timeframes.

(xix) Ensure that incidents of invoice disputes are continually updated, at a minimum on a weekly basis.

(xx) Keep the MSI informed of activity and anticipated resolution times for active incidents of invoice disputes.

(xxi) Allow DIR to monitor and validate invoice dispute process on an ongoing basis.

(xxii) Provide a process for escalating to Successful Respondent management incidents of invoice disputes not resolved within the time frames established within DIR policies.

(xxiii) Provide data to enable the MSI to report on all DCS financial items, including, at a minimum:

A. Provide application transaction and financial transaction data to the MSI to enable the MSI provided Financial Management System functionality to allow for near real-time reporting of the DCS transaction and payment details including reports as required to fully reconcile all attempted and failed transactions.

B. Provide customer, application and transaction data to the MSI as required to enable the MSI provided reporting on transactions and payment data by type of transaction, application, customer, etc.

C. Provide the required data to the MSI with the appropriate level of detail to enable the MSI to link all financial items to each individual transaction.

D. Provide the required data to the MSI to enable the MSI to invoice DCS Customers for DCS fees.

# 10. Contract Management

## 10.1. Contract Changes

(a) Any change or modification to the Agreement that alters pricing, the material terms of the Agreement, or alters Articles 1 through 14 of the Agreement must be made by a properly executed Contract amendment.

(b) Other changes or modifications to the Agreement may be made through the appropriate contract change process and shall occur in accordance with the relevant SMM.

## 10.2. Deliverables

(a) Deliverables may have certain attributes that impact the review and acceptance.

(b) The attributes for each of the Deliverables are detailed in **Attachment 1.1 Deliverables** and with definitions summarized below.

(c) Critical (C) (flagged within the Agreement and referenced in **Attachment 1.1 Deliverables**). Deliverables that are Critical have associated Deliverable Credits payable to DIR in the event Successful Respondent fails to successfully complete and submit such Deliverables to DIR on or before the due dates identified in **Attachment 1.1 Deliverables**. For further clarity, successfulness is measured by whether the Deliverables meet the associated Acceptance Criteria.

(d) Payment (P) Payment Deliverables are the deliverables that have associated payments due to the Successful Respondent after DIR approval of such deliverables. Payment will be provided in accordance with **Exhibit 2 Pricing**.

(e) Time-critical (T) – Deliverables that are designated as time-critical will have an expedited review period of five (5) Business Days.

(f) For avoidance of doubt, a specific Deliverable's attributes may be changed upon mutual agreement and through the appropriate contract change request process as determined by the material nature of changes.

(g) Project Milestones. DIR or DCS Customers shall have the right to review and accept or reject the milestones in accordance with the SMM.

## 10.3. Deliverable Acceptance Criteria

(a) In order to eliminate the potential for frequent submission and rejection of Deliverables, the Successful Respondent shall meet with DIR and reach agreement on the construct and content for Deliverables prior to creation. The Successful Respondent shall coordinate fully and appropriately with DIR and its partners throughout the development of Deliverables and reviews of deliverables prior to formal submission as requested. At a minimum, Deliverables shall meet the acceptance criteria defined in **Attachment 1.1 Deliverables**. Unless otherwise agreed, and as applicable, Successful Respondent shall perform comprehensive testing (e.g., unit, string, integration, stress, volume, system testing) on each such Deliverable prior to submitting such item to DIR for Acceptance. DIR considers the Deliverable due date to be the day by which the Deliverable is ready for acceptance and formally submitted.

(b) The Successful Respondent shall use the SMM process to formally submit final versions of the Deliverables to DIR.

(c) For all Deliverables, the Successful Respondent shall comply with the following requirements:

(i) The Successful Respondent shall follow all DIR-prescribed processes and procedures and SMMs;
(ii) The Successful Respondent shall provide actionable Deliverables which successfully meet all requirements outlined in the Agreement;
(iii) The Successful Respondent shall deliver all Deliverables in accordance with the DIR-approved Deliverable schedule;
(iv) The Successful Respondent shall correct any latent defects identified after the acceptance of a Deliverable at no additional cost to DIR;
(v) The Successful Respondent shall comply with specific acceptance criteria detailed in the Agreement and referenced in **Attachment 1.1 Deliverables.**

## 10.4. Deliverable Expectation Document (DED)

(a) At DIR's discretion, a DED may be used for Deliverables to document mutually agreed upon Deliverable descriptions, applicable standards, and more clearly define Acceptance Criteria previously documented in **Attachment 1.1 Deliverables**. The Successful Respondent and DIR will develop and mutually agree on DEDs. Deliverable acceptance will be contingent on material compliance with the DED and any rejection of a Deliverable must be accompanied by a description of the material non-compliance with the DED. DIR, in its sole discretion, may choose to forgo the creation of the DED.

(b) The DEDs shall not contradict nor alter the Contract Acceptance Criteria requirements set forth in the Agreement or in **Attachment 1.1 Deliverables**. In the absence of a DED, the Acceptance Criteria for a Deliverable would be material compliance with the requirements as set forth in the Agreement or in **Attachment 1.1 Deliverables**.

(c) There may be situations where agile development of deliverables may be appropriate. In such cases, the Acceptance Criteria in **Attachment 1.1 Deliverables,** for a Deliverable may be described at a high level and the DED may be used to capture requirements for a sprint or series of sprints.

(d) Any changes to the DED will be approved through mutual agreement between DIR and the Successful Respondent.

(e) The following requirements may be documented in the DEDs:

(i) Format of the Deliverables;
(ii) Deliverable Description;
(iii) Submission Process and Requirements;
(iv) Delivery Schedule including Incremental Delivery Dates, if applicable;
(v) Review and Comment Requirements (who, when, how); and
(vi) Acceptance Criteria.

## 10.5. Deliverables Review Meeting

The status of each Deliverable and any associated issues will be managed through a Deliverables review meeting between DIR and the Successful Respondent. The objective of the meeting is to review the status of Deliverables, communicate Deliverable owners and Deliverable recipients for upcoming Deliverables, review non-compliant deliverables and remediation plans for those Deliverables as needed.

## 10.6. Acceptance Review Period

(a) It is critical to the success of the Successful Respondent that the deliverable acceptance process is thorough and that any deficiencies are addressed as early as possible to minimize impacts to the Services. Designated DIR working teams will be reviewing the Deliverables throughout the phases of development. Successful Respondent will solicit input from DIR as the Deliverables are developed. The Successful Respondent shall review the expectations in advance so as to obtain acceptance of the final Deliverable within the Acceptance Review Period.Feedback and suggestions received from DIR will be incorporated into the Deliverable.

(b) There may be deliverables within the Contract that are designated to have a "parent/child" relationship with another Service Component Provider. For those specific deliverables, the review and acceptance periods will follow the "parent" deliverable.

(c) DIR will notify the Successful Respondent, in writing, within ten (10) Business Days, or such other time as may be mutually agreed to considering the size, criticality, and complexity of the Deliverable, or as may be designated as Time-Critical (TC) in **Attachment 1.1 Deliverables,** of the acceptance or non-acceptance of the Deliverable. During this Acceptance Review Period, DIR shall review and may further test each Deliverable, individually and/or collectively, to determine whether such item(s) comply with Acceptance criteria. Successful Respondent shall cooperate with such review and testing efforts, provide a technical environment to facilitate such review, and provide all applicable documentation that may assist in such review and testing. DIR will notify the Successful Respondent of any deficiencies that must be corrected prior to acceptance.

(d) If the Successful Respondent does not receive written notice from DIR by the end of the review period, the Successful Respondent may notify DIR in writing that DIR has five (5) additional Business Days to provide written notice. The Deliverable will be deemed to be accepted by DIR if DIR does not provide such notice of acceptance or non-acceptance at the end of this additional five (5) Business Day period.

(e) If DIR does not provide notice of Acceptance or deliver a notice of Noncompliance to Successful Respondent by the end of the Acceptance Review Period, DIR may request in writing an additional Acceptance Review Period to be mutually agreed to by both parties. Should DIR require additional time to review the Deliverable and has not received notice from the Successful Respondent regarding the additional Acceptance Review Period of five (5) Business Days, DIR may provide notice to the Successful Respondent that an extension of the DIR review period is needed. Successful Respondent and DIR shall work together to establish a revised acceptance review period.

(f) Neither DIR's nor any DCS Customer's use in a live production environment shall constitute Acceptance, affect any rights and remedies that may be available to DIR or a DCS Customer, and/or

constitute or result in "acceptance" under general contract Laws, the State's Uniform Commercial Code or any other Laws.

### 10.7. Noncompliance

(a) If DIR delivers to the Successful Respondent a written notice of non-compliance, the Successful Respondent shall correct all deficiencies identified in DIR's notice and within five (5) Business Days for written Deliverables, or such other time as mutually agreed to, at no additional charge to DIR. Beginning upon receipt of notice from Successful Respondent that the Deliverable resubmission is ready to be Accepted, an Acceptance Review Period of ten (10) Business Days shall begin again and the Parties shall perform their obligations as described above in Acceptance Review Period.

(b) For deliverables that are Time-Critical as designated in **Attachment 1.1 Deliverables,** within two (2) Business Days or as otherwise mutually agreed, after receiving such notice from DIR, and at no charge to DIR, Successful Respondent shall correct such Noncompliance, satisfy the Acceptance Criteria as outlined in the Noncompliance notification. Beginning upon receipt of notice from Successful Respondent that a Deliverable resubmission is ready to be Accepted, an Acceptance Review Period of two (2) Business Days or as otherwise mutually agreed, shall begin and the Parties shall perform their obligations under Section 10.6 Acceptance Review Period above.

### 10.8. Failure to Cure a Noncompliance

(a) If Successful Respondent:

(i) requires more than two (2) attempts to cure a particular Noncompliance;
(ii) does not correct a Noncompliance within the timeframes defined in the Section 10.6 Acceptance Review Period; or
(iii) cures a particular Noncompliance and such cure results in another Noncompliance and Successful Respondent is not able to collectively cure such Noncompliance(s) within one (1) attempt in five (5) Business Days

(b) then DIR may, in its sole discretion, apply any remedies including, but not limited to Deliverable Credits.

(c) After pursuing the cure process stated above, upon written notification to Successful Respondent, DIR in its sole discretion may choose to forgo assessing any remedies, including but not limited to Deliverables Credits and may choose to:

(i) conditionally Accept the Deliverable and require Successful Respondent to develop a remediation plan, subject to DIR's acceptance and within timeframes reasonably requested by DIR whereby Successful Respondent shall design and implement a workaround solution that mitigates the Noncompliance;
(ii) correct the Noncompliance itself or hire a third party to correct the Noncompliance at Successful Respondent's expense (all such out-of-pocket expenses and costs of DIR and/or the DCS Customer to be subject to set-off as set forth in **Exhibit 2 Pricing** requirements related to Set Off);
(iii) implement and use the Deliverable despite the Noncompliance and equitably reduce the Charges; and/or

(iv) exercise any of its other rights under this Agreement or available at law or in equity, including the right to reject any Deliverable.

(d) The remedies above are in addition to and shall not limit DIR's other remedies, whether at Law, in equity, or under this Agreement.

### 10.9. Remediation of Defects in Previously Accepted Items

(a) In the event of a discovery of a latent defect in a previously Accepted Deliverable or other Deliverable, where such latent defect would have qualified as a Noncompliance at the time of Acceptance, upon discovery, the Successful Respondent will, at no additional charge, repair or replace or otherwise correct the Noncompliance to the level of performance specified in the Agreement.

(b) Further, should any modification or rework of a previously Accepted Deliverable or other Deliverable be required for Acceptance of a subsequent deliverable, then Successful Respondent shall perform such modification or rework at no charge and each Party's obligations, rights, and remedies described herein shall continue to apply.

### 10.10. Deliverables Credits

Successful Respondent recognizes that DIR is paying Successful Respondent to provide certain Critical Deliverables by the time and in the manner agreed by the Parties. If Successful Respondent fails to meet its obligations with respect to such Critical Deliverables, then, in addition to other remedies available to DIR, Successful Respondent shall pay or credit to DIR the amounts specified in Article 6 Performance Model – Service Level Agreements as applicable, or established by DIR as part of the Project approval process on a case by case basis in recognition of the diminished value of the Services resulting from Successful Respondent's failure to meet the agreed upon level of performance, and not as a penalty (the "**Deliverable Credits**"). If DIR recovers monetary damages from Successful Respondent as a result of Successful Respondent's failure to meet its obligations with respect to one (1) or more Critical Deliverables, Successful Respondent shall be entitled to set-off against such damages any Deliverable Credits paid for the failures giving rise to such recovery. Deliverable Credits are distinct from Service Level Credits and shall not be counted toward or subject to the overall cap on Successful Respondent's liability.

## 11. Contract Conclusion Requirements: Transition at Contract Termination or Non-Renewal

### 11.1. Overview

(a) Successful Respondent will provide to the State the Termination Assistance Services set forth herein in connection with the termination or expiration of the Contract.

(b) To the extent the Termination Assistance Services include any tasks which Successful Respondent is not otherwise obligated to perform under the Contract, the charges will be based on then-current rates for Services as proposed by Successful Respondent in this Exhibit or prevailing rates at the time of termination, whichever is lower.

(c) "Termination Assistance Services" will mean:

(i) to the extent requested by the State, the continued performance by Successful Respondent of its obligations under the Contract (including providing the Services which are subject to termination or expiration), and

(ii) the provisioning of such assistance, cooperation and information as is reasonably necessary to help enable a smooth transition of the applicable Services to the State or its designated 3rd Party provider ("Successor").

(d) As part of Termination Assistance Services, Successful Respondent will provide such information as the State may reasonably request relating to the number and function of each of the Successful Respondent personnel performing the Services, and Successful Respondent will make such information available to the Successor designated by the State.

(e) Successful Respondent will cooperate with the State in its attempts at transferring the services responsibilities to another provider in a manner in keeping with not adversely affect the provision of ongoing services.

## 11.2. Termination Assistance Services

### 11.2.1. General

Upon DIR's request, Successful Respondent shall provide Termination Assistance Services directly to DIR, any DCS Customer, any successors or assignees of such Entities and any of their designee(s).

#### 11.2.1.1. Period of Provision

Successful Respondent shall provide Termination Assistance Services commencing on the date a determination is made by DIR that there shall be an Assistance Event, which date may be up to twenty-four (24) months prior to effective date of such Assistance Event or on such earlier date as DIR may request, and continuing for up to three (3) months after the effective date of such Assistance Event, as designated by DIR, subject to such further extensions as permitted in **MSA, Section 4.2 Use of Third Parties**.

#### 11.2.1.2. Notice of an Assistance Event

DIR will provide Successful Respondent with written notice of an Assistance Event. Such notice will include a description of the Services that are to be terminated or discontinued, the affected DCS Customers, and the anticipated effective date of the Assistance Event. DIR may modify or update any of the information provided in the initial notice of an Assistance Event from time to time by a supplemental notice from DIR to Successful Respondent.

#### 11.2.1.3. Extension of Termination Assistance Services

DIR may elect to end the period for performance of Termination Assistance Services (in whole or in part), in its sole discretion, and restart the period for performance of Termination Assistance Services provided that the total of all such delays shall not result in Termination Assistance Services being performed for no more than a total of twenty-seven (27) months without Successful Respondent's consent.

#### 11.2.1.4. Firm Commitment

Successful Respondent shall provide Termination Assistance Services regardless of the reason for the Assistance Event (including a termination for cause by Successful Respondent).

#### 11.2.1.5. Performance

Successful Respondent shall provide all Termination Assistance Services subject to and in accordance with the terms and conditions of this Agreement. Successful Respondent shall perform Termination Assistance Services with at least the same degree of accuracy, quality, completeness, timeliness, responsiveness and resource efficiency as it is or was required to provide the same or similar Services in accordance with this Agreement. The quality and level of performance of Termination Assistance Services provided by Successful Respondent shall continue to meet or exceed the Service Levels and shall not be degraded or deficient in any respect. Service Level Credits shall be assessed for any failure to meet Service Levels during any period in which Termination Assistance Services are provided. If any period for performing any Termination Assistance Services extends beyond the expiration or the effective date of any termination of this Agreement, the provisions of this Agreement shall remain in full effect for the duration of such period.

### 11.2.2. Scope

As part of the Termination Assistance Services, Successful Respondent shall timely transfer the control and responsibility for Services previously performed by or for Successful Respondent to DIR, the DCS Customers and/or their designee(s), and upon DIR request, shall execute any documents reasonably necessary to affect such transfers. Successful Respondent shall also provide any and all information and assistance requested by DIR required for:

(i) the Systems and processes associated with the Services to operate and be maintained and enhanced efficiently;
(ii) the Services to continue without interruption or adverse effect; and
(iii) the orderly transfer of the Services (or replacement or supplemental services) to DIR, the DCS Customers and/or their designee(s).

### 11.2.3. General Support

(a) Prior to the Termination Assistance event, Successful Respondent shall:

(i) assist DIR, the DCS Customers and/or their designee(s) in developing a written plan for the migration of the Services to DIR, the DCS Customers and/or their designee(s), which plan shall include (as requested by DIR) capacity planning, process planning, facilities planning, human resources planning, technology planning, telecommunications planning and other planning necessary to effect the transition,
(ii) perform programming and consulting services as requested to assist solely in implementing the transition plan,
(iii) train personnel designated by DIR, the DCS Customers and/or their designee(s) in the use of any processes or associated Equipment, Materials, Systems or tools used in connection with the provision of the Services as needed for such personnel to assume responsibility for performance of the Services,
(iv) provide a catalog of all processes, Materials, DIR Data, Equipment, Third Party Contracts, automation scripts, and tools used to provide the Services,

(v) provide machine readable and printed listings and associated documentation for source code for Software owned by DIR or any DCS Customer and source code to which DIR and/or the DCS Customers are entitled under this Agreement and assist in its re-configuration,
(vi) provide technical documentation for Software used by Successful Respondent to provide the Services as needed for continuing performance of the Services,
(vii) analyze and report on the space required for the DIR Data and the Software needed to provide the Services,
(viii) assist in the execution of data migration and testing process until the successful completion of the transition to DIR, the DCS Customers and/or their designee(s),
(ix) create and provide copies of the DIR Data in the format and on the media requested by DIR, the DCS Customers and/or their designee(s),
(x) provide a complete and up-to-date, electronic copy of the Service Management Manual (SMM) in the format and on the media requested by DIR, the DCS Customers and/or their designee(s), and
(xi) provide other technical and process assistance, documentation and information as requested by DIR, the DCS Customers and/or their designee(s).

(b) After the Assistance Event and during the Termination Assistance Period, Successful Respondent shall answer any questions that may arise concerning the Services previously performed by the Successful Respondent. DIR may request Successful Respondent to provide certain discontinued Services after the Assistance Event; however, such Termination Assistance Services may include a charge as described in Section 11.2.12 Rates and Charges.

### 11.2.4. Certain Materials

(a) Successful Respondent shall provide source code and artifacts (e.g., documentation, use cases, test scripts, design models, activity diagrams and systems configuration) which Successful Respondent has in its possession, or Successful Respondent Agents have in their possession, for:

(i) any modification or enhancement made hereunder by Successful Respondent to DIR Software,
(ii) any Software developed pursuant to this Agreement which DIR owns or with respect to which DIR is otherwise entitled to source code, and
(iii) as otherwise provided in an applicable Statement of Work;

(b) Successful Respondent shall provide such source code and artifacts:

(i) upon any request from DIR during the Term and any Termination Assistance Period,
(ii) upon termination or expiration of this Agreement or the applicable Statement of Work, and
(iii) upon the End Date.

### 11.2.5. Right to Acquire

DIR, the DCS Customers and/or their designee(s) shall have the right (but not the obligation) to purchase any or all Software as a Service (SaaS) type systems and on premise software licenses that are owned by

Successful Respondent and implicated by the relevant Assistance Event subject to the requirements set forth in **MSA, Sections 4.12.1 and 4.16.3**.

### 11.2.6. Personnel

#### 11.2.6.1. List of Successful Respondent Personnel

Successful Respondent shall promptly provide to DIR a list, organized by location, of the Successful Respondent Personnel assigned to the performance of the Services that are implicated by each Assistance Event. Such list shall, subject to applicable Privacy Laws, specify each such Successful Respondent Personnel's name, job title, compensation package, leave status, years of service and job responsibilities. DIR agrees not to disseminate the personally identifiable information contained in such list without Successful Respondent's consent. Successful Respondent shall not terminate, reassign or otherwise remove from the performance of the Services any such dedicated Successful Respondent Personnel until after the end of the applicable Termination Assistance Services period.

#### 11.2.6.2. Right to Hire

(a) DIR, the DCS Customers and/or their designee(s) shall be permitted, without interference (including through counter-offers) from Successful Respondent (subject to this section), to meet with, solicit and hire, effective after the later of:

(i) the date of DIR's notice of an Assistance Event, and

(ii) the completion of the Termination Assistance Services requiring such Successful Respondent Personnel, any Successful Respondent Personnel substantially dedicated to the performance of the Services during the twelve (12) month period prior to the date of DIR's notice of an Assistance Event who are implicated by that Assistance Event.

(b) Successful Respondent hereby waives its rights, if any, under contracts with such Successful Respondent Personnel restricting the ability of such Successful Respondent Personnel to be recruited or hired by DIR, the DCS Customers and/or their designee(s) (including waiving any right to restrict such personnel via non-compete agreements or other contractual means). Successful Respondent will provide DIR, the DCS Customers and/or their designee(s) with reasonable assistance in their efforts to meet with, solicit and hire such Successful Respondent Personnel, and will give DIR, the DCS Customers and/or their designee(s) reasonable access to such Successful Respondent Personnel for interviews, evaluations and recruitment. DIR shall endeavor and shall cause the DCS Customers and their designee(s) to endeavor, to conduct the above-described activities in a manner that is not unnecessarily disruptive of Successful Respondent's performance of its obligations under this Agreement.

#### 11.2.6.3. Subcontractor Employees

(a) With respect to Subcontractors, Successful Respondent shall:

(i) obtain for DIR, the DCS Customers and their designee(s) the rights specified in Section 11.2.6.2 Right to Hire, and

(ii) ensure that such rights are not subject to subsequent Subcontractor approval or the payment of any fees, charges or other amounts.

(b) If Successful Respondent is unable to obtain any such rights with respect to a Subcontractor, it shall notify DIR in advance and Successful Respondent shall not subcontract any Services to such Subcontractor without DIR's prior approval (and absent such approval, Successful Respondent's use of any such Subcontractor shall obligate Successful Respondent to obtain or arrange, at no additional cost to DIR, the rights specified in Section 11.2.6.2 Right to Hire, for DIR, the DCS Customers and their designee(s)).

### 11.2.7. Materials

DIR shall have the rights and licenses set forth in Section 11.2.9 DIR Facilities, Equipment, and Materials and Section 11.2.8.2 Right to Acquire in respect of Successful Respondent Owned Materials and Third Party Materials.

### 11.2.8. Equipment

#### 11.2.8.1. List of Equipment

Successful Respondent shall promptly provide to DIR a list, organized by location, of the Equipment that is implicated by each Assistance Event. Such list shall specify information requested by DIR, including all fields tracked by Successful Respondent in any asset management system used by Successful Respondent for tracking and managing Equipment, such Equipment's function, manufacturer, model number, age, and other pertinent information.

#### 11.2.8.2. Right to Acquire

DIR, the DCS Customers and/or their designee(s) shall have the right (but not the obligation) to purchase or (subject to Section 11.2.9 DIR Facilities, Equipment, and Materials) assume the lease for any or all Equipment that is owned or leased by Successful Respondent and that is implicated by the relevant Assistance Event. Subject to Section 11.2.9 DIR Facilities, Equipment, and Materials, such Equipment shall be transferred in good working condition, reasonable wear and tear excepted, as of the later of the effective date of the relevant Assistance Event and the completion of the Termination Assistance Services requiring such Equipment. Successful Respondent shall maintain such Equipment through the date of transfer so as to be eligible for the applicable manufacturer's maintenance program. In the case of Successful Respondent-owned Equipment (including Equipment owned by Successful Respondent Affiliates and Subcontractors and further including any such Equipment leased to Successful Respondent), Successful Respondent (or such Affiliate or Subcontractor) shall grant to DIR, the DCS Customers, and/or their designee(s) a warranty of title and a warranty that such Equipment is free and clear of all liens, security interests, and other encumbrances. Such conveyance by Successful Respondent (or Affiliate or Subcontractor) to DIR, the DCS Customers, and/or their designee(s) shall be at fair market value (as shall be determined by an agreed-upon appraisal); provided, however, in the case of any item of Equipment for which the acquisition cost has been the basis of Charges to DIR (e.g., as in the case of the Hardware Service Charge provided in **Exhibit 2 Pricing**), such conveyance shall be at an amount not exceeding the amount of any then unrecovered acquisition cost computed in accordance with the method used to charge DIR therefor. At DIR's request, the Parties shall negotiate in good faith

and agree upon the form and structure of the purchase. In the case of leased Equipment, Successful Respondent shall:

(i) represent and warrant that the lease is not in default,
(ii) represent and warrant that all payments thereunder have been made through the date of transfer, and
(iii) notify DIR, the DCS Customers, and/or their designee(s) of any lessor defaults of which it is aware at the time.

### 11.2.9. DIR Facilities, Equipment, and Materials

Successful Respondent shall vacate the DIR Facilities and return to DIR, if not previously returned, any resources that are implicated by the relevant Assistance Event and that are owned, leased or licensed by DIR, any DCS Customer, or any DIR Contractor, including DIR owned or leased Equipment, DIR Owned Materials and DIR licensed Materials, in condition at least as good as the condition of such facilities and resources when they were made available to Successful Respondent, ordinary wear and tear excepted. Such facilities and resources shall be vacated and/or returned as of the later of the effective date of the relevant Assistance Event and the completion of the Termination Assistance Services requiring such facilities or resources.

### 11.2.10. Third Party Contracts

Successful Respondent shall promptly, but no less than thirty (30) days from DIR's issuance of notice of an Assistance Event, provide to DIR a list of the Third Party Contracts that are implicated by the relevant Assistance Event. At any time during the contract term, DIR may request and Successful Respondent shall provide the Third Party Contract(s) in accordance with **MSA, Section 4.16.3**, regardless of whether Successful Respondent's other customers utilize or benefit from such Third Party Contract(s). Except for the Third Party Contracts specified in **Exhibit 2 Pricing**, in accordance with **MSA, Section 4.16.3** subject to Section 11.2.9 DIR Facilities, Equipment, and Materials, Successful Respondent shall, at DIR's request, cause the counter-parties to such Third Party Contracts to permit DIR, the DCS Customers, and/or their designee(s) to assume prospectively any or all such Third Party Contracts or to enter into new contracts with DIR, the DCS Customers, and/or their designees on substantially the same terms and conditions, including price. Successful Respondent shall transfer or assign those Third Party Contracts that DIR elects to assume prospectively to DIR, the DCS Customers, and/or their designee(s) as of the later of the effective date of the relevant Assistance Event and the completion of the Termination Assistance Services requiring such Third Party Contracts. Such transfers or assignments shall be on terms and conditions acceptable to all applicable parties, provided that:

(i) there shall be no fee, charge or other amount imposed on DIR, the DCS Customers, and/or their designee(s) by Successful Respondent or the counter-parties to such Third Party Contracts for such transfer or assignment, and
(ii) Successful Respondent shall:
    A. promptly cure and, in accordance with **MSA, Section 10.1.3 Licenses, Leases, and Contracts**, indemnify DIR against any default under such Third Party Contracts relating to the period prior to such transfer or assignment;
    B. represent and warrant that all payments thereunder through the date of transfer or assignment are current; and

C. notify DIR, the DCS Customers, and/or their designee(s) of any counter-party's default with respect to such Third Party Contracts of which it is aware at the time of such transfer or assignment.

### 11.2.11. Other Subcontracts and Third Party Contracts

With respect to Third Party Contracts implicated by the relevant Assistance Event that are not otherwise transferred or assigned to DIR, the DCS Customers, and/or their designee(s) pursuant to **MSA, Section 4.2.2 Successful Respondent Cooperation**, Successful Respondent shall make available to DIR, the DCS Customers, and/or their designee(s), pursuant to reasonable terms and conditions, any Third Party services then being utilized by Successful Respondent in the performance of the Services. Successful Respondent shall retain the right to utilize any such Third Party services in connection with the performance of services for other Successful Respondent customers. DIR and the DCS Customers shall retain the right to contract directly with any third party previously utilized by Successful Respondent to perform any Services.

### 11.2.12. Rates and Charges

(a) Except as provided in this Subsection and **MSA, Section 4.2.2 Successful Respondent Cooperation**, Successful Respondent shall provide all Termination Assistance Services at no additional charge. The Parties anticipate that Termination Assistance Services requested by DIR shall be provided by Successful Respondent using Successful Respondent Personnel already assigned to the performance of the Services and without adversely affecting Successful Respondent's ability to meet its performance obligations. To the extent DIR requests that Successful Respondent perform only a portion (but not all) of the Services included in a particular Charge, the amount to be paid by DIR shall be equitably adjusted downward in accordance with **Exhibit 2 Pricing**, to the extent applicable, or equitably adjusted downward in proportion to the portion of the Services that Successful Respondent shall not be providing to the extent that **Exhibit 2 Pricing** does not provide for such reduction. If and to the extent Termination Assistance Services requested by DIR cannot be provided by Successful Respondent using Successful Respondent Personnel then-assigned to the performance of the Services without adversely affecting Successful Respondent's ability to meet its performance obligations, DIR, in its sole discretion, may:

(i) forego or delay any work activities or temporarily or permanently adjust the work to be performed by Successful Respondent, the schedules associated therewith or the Service Levels to permit the performance of such Termination Assistance Services using such personnel, or

(ii) authorize Successful Respondent to use additional Successful Respondent Personnel to perform Termination Assistance Services.

(b) To the extent DIR authorizes Successful Respondent to use additional Successful Respondent Personnel to perform Termination Assistance Services requested by DIR, DIR shall pay Successful Respondent the applicable rates and charges specified in **Exhibit 2 Pricing** for such Full-time Positions (FTPs) or Full-time Equivalents (FTEs) or, if no such rates and fees are specified in **Exhibit 2 Pricing**, a negotiated fee for the additional Successful Respondent Personnel required to perform such Termination Assistance Services (determined on the basis of pricing no less favorable to DIR than the pricing and labor rates set forth herein for comparable Services), provided that Successful

Respondent notifies DIR in advance of any such charges, obtains DIR's approval prior to incurring such charges, and uses commercially reasonable efforts to minimize such charges. Notwithstanding the foregoing, DIR will not be obligated to pay Successful Respondent for any such additional Successful Respondent Personnel if at any time prior to DIR's issuance of the notice of Assistance Event, Successful Respondent failed to sufficiently staff the Services that are the subject of the Assistance Event (both with respect to number of personnel and personnel with the necessary skills and training).

#### 11.2.13. Proprietary Communications Network

If Successful Respondent uses a proprietary communications network to provide the Services, then for a period of up to two (2) years following the effective date of the relevant Assistance Event, Successful Respondent shall, if requested by DIR, continue to provide such proprietary communications network and other network Services to DIR, the DCS Customers, and/or their designee at the rates, and subject to the terms and conditions, set forth in this Agreement.

#### 11.2.14. Information

Upon the occurrence of any breach by Successful Respondent under this Agreement or if DIR elects to evaluate re-procurement of all or any portion of the Services, Successful Respondent will provide to and/or make available for DIR review any and all reports, data and information that DIR deems necessary in order to evaluate all options related to such breach and/or re-procurement, including without limitation, all reports, data and information specified in **MSA, Section 4.2.1 Right of Use**. For the avoidance of doubt, Successful Respondent will be obligated to provide all such reports, data and information regardless of whether DIR has provided notice of or otherwise declared an Assistance Event.

### 11.3. Successful Respondent Sourced and Managed Contracts

(a) The Successful Respondent shall ensure that all Successful Respondent-sourced contracts inclusive of general building maintenance and repairs, telecommunications, environmental testing, facility mechanical maintenance (e.g., UPS and diesel/fuel power generation) that do not support DCS Customer operations are terminated (save for those contracts that DIR assumes or those that DIR requires the Successful Respondent assign or transfer to DIR or its designee), and that DIR is not obligated to any ongoing financial, contractual or other obligations associated with these contracts or any Successful Respondent or third-party services, equipment or maintenance that support these contracts.

(b) The Successful Respondent shall transfer the terminated or expired Services to DIR or its designee(s)/successor(s) in an efficient and orderly manner.

(c) Prior to such actions being taken, the Successful Respondent shall verify with DIR that the impact on DIR's business (including its personnel and customers) and the internal and third-party IT-related costs incurred by DIR in transferring the terminated services are acceptable to DIR under the circumstances.

(d) The Successful Respondent shall continue to perform such services without disruption or deterioration until the transfer has occurred:

(i) consistent with the terms and conditions of this Contract, or

(ii) except as approved by DIR.

(e) In an effort to facilitate transition of responsibilities, the Key Management Position obligations in the Section 5.7 Evergreen Service Personnel will continue to apply during the agreed Termination Assistance Period.

## 11.4. Termination Assistance Plan

The contents of Termination Assistance Plan will include, unless otherwise agreed, the services, functions, and activities as defined below:

(i) Documentation of existing and planned Projects and support activities;
(ii) Identification of the Services and related positions or functions that require transition and a schedule, plan and procedures for the State or its designee assuming or reassuming responsibility;
(iii) Description of actions to be taken by Successful Respondent in performing Termination Assistance;
(iv) Description of how the transfer of:
  A. relevant information regarding the Services,
  B. resources (if any),
  C. operations, and
  D. contracts (if any) will be achieved;
(v) Description in detail of any dependencies on the successors necessary for Successful Respondent to perform the Termination Assistance Services (including an estimate of the specific Successful Respondent staffing required);
(vi) Inventory of documentation and work products required to facilitate the transition of responsibilities;
(vii) Assist the State in the identification of significant potential risk factors relating to the transition and in designing plans and contingencies to help mitigate the risk;
(viii) Set out the timeline for the transfer of each component of the terminated Services (including key milestones to track the progress of the transfer); and
(ix) Define a schedule and plan for Successful Respondent's return to the State of:
  A. the State Service locations then occupied by Successful Respondent (if any), and
  B. the State Confidential Information, the State Data, documents, records, files, tapes and disks in Successful Respondent's possession.

## 11.5. Termination Management Team

(a) The Successful Respondent will provide a senior Project manager who will be responsible for Successful Respondent's overall performance of the termination assistance services and who will be the primary point of contact for the State in respect of the termination assistance services during the termination assistance period.

(b) DIR will appoint a senior Project manager who will be the primary point of contact for Successful Respondent during the termination assistance period. Additionally, DIR may appoint a transformation team that would be responsible for the review of then current services provided by the Successful Respondent and work to facilitate an orderly transition of services.

### 11.6. Operational Transfer

(a) Successful Respondent will perform the activities reasonably required to help effect a smooth and orderly transfer of operational responsibility for the Terminated Services.

(i) Facilitating access to the State source code, object code, object and production libraries, reference files, field descriptions, record layouts and technical specifications along with run documentation for the State software then in Successful Respondent's possession including tools, scripts, SMMs, production schedules and procedures as required to support the in-scope applications which may be used in training, knowledge transfer, sizing assessments, operational reviews and other uses required by the state at the time of transfer.

(ii) Cooperate with the Successors in conducting migration testing.

(iii) Providing the DIR-owned documents and information related to the functionality, program code, data model and database structure, and access methods for the in-scope applications and manual and automated processes used for the State, within the possession or control of Successful Respondent, and reviewing such processes, documents and information with the Successor as reasonably requested.

(iv) Cooperate with the State's test plans, back out procedures, and contingency plans as part of the migration of terminated services.

(b) After the transfer of the provision of Terminated Services to the State, its designee(s), or both, providing additional assistance as reasonably requested by the State to facilitate continuity of operations, through the end of the Termination Assistance Period.

## 12. Other Requirements

### 12.1. Support Requirements

(a) The Successful Respondent must describe the support it wants from the State other than what the State has offered in the Proposal document. Specifically, the Respondent must address the following:

(i) Nature and extent of State support required in terms of staff roles, percentage of time available, and so on;

(ii) Assistance from State staff and the experience and qualification levels required; and

(iii) Other support requirements.

(b) DIR may not be able or willing to provide the additional support the Respondent lists in this part of its Proposal. The Respondent therefore must indicate whether its request for additional support is a requirement for its performance. If any part of the list is a requirement, DIR may reject the Respondent's Proposal, if the State is unable or unwilling to meet the requirements.

### 12.2. Materials

Successful Respondent shall not utilize any Successful Respondent Owned Materials that are not commercially available.

**<End of Statement of Work>**